SUPREME COURT OF INDIA

CIVIL WRIT PETITION 829 / 2013

IN THE MATTER OF:

S.G. VOMBATKERE & ANR. ...PETITIONERS

Versus

UNION OF INDIA & ORS. ...RESPONDENTS

COMPILATION

VOLUME V - A

UIDAI & NPR DOCUMENTS

(Pages 1 - 216)

(See Inside for Complete Index)

Submitted on behalf of the Petitioners

VOLUME V

UIDAI & NPR DOCUMENTS

1
2

Annexure X

(TO BE PUBLISHED IN PART-I, SECTION-2 OF THE GAZETTE OF INDIA)

GOVERNMENT OF INDIA
PLANNING COMMISSION

Yojana Bhawan, Sansad Marg,
New Delhi, 28th January,2009

NOTIFICATION

No. A-43011/02/2009-Admn.I: In pursuance of Empowered Group of Ministers' fourth meeting, dated 4th November 2008, the **Unique Identification Authority of India (UIDAI)** is hereby constituted and notified as an attached office under aegis of Planning Commission with following terms of reference and initial core staff composition:-

COMPOSITION:

2. UIDAI shall be set up with an initial core team of 115 officials and staff as per details given below:

Post	Level	No. of Posts
UID Authority of India		
Director General & Mission Director	Additional Secretary Govt. of India	1
Deputy Director General (DDG)	Joint Secretary, Govt. of India	1
Assistant Director General (ADG)	Director, Govt. of India	1
Support Staff		
PS	PS	3
Peon	Peon	2
Driver	Driver	2
	Total Manpower	10
State /UT Units of UIDAI		
State / UT UID Commissioner	Joint Secretary, Govt. of India	35
Support Staff		
PS	PS	35
Peon	Peon	35
	Total Manpower	105
Grand Total		115

Annexure 1

Role and Responsibilities of UIDAI

3 UIDAI shall have the responsibility to lay down plan and policies to implement UID Scheme, shall own and operate UID database and be responsible for its updation and maintenance on an ongoing basis.

4 Implementation of UID scheme will entail, *inter alia*, following responsibilities being undertaken by UIDAI:

- Generate and assign UID to residents
- Define mechanisms and processes for interlinking UID with partner databases on a continuous basis
- Frame policies and administrative procedures related to updation mechanism and maintenance of UID database on an ongoing basis
- Co-ordinate / liaise with implementation partners and user agencies as also define conflict resolution mechanism
- Define usage and applicability of UID for delivery of various services
- Operate and manage all stages of UID lifecycle
- Adopt phased approach for implementation of UID specially with reference to approved timelines
- Take necessary steps to ensure collation of NPR with UID (as per approved strategy)
- Ensure ways for leveraging field level institutions appropriately such as PRIs in establishing linkages across partner agencies as well as its validation while cross linking with other designated agencies
- Evolve strategy for awareness and communication of UID and its usage
- Identify new partner /user agencies
- Issue necessary instructions to agencies that undertake creation of databases, to ensure standardization of data elements that are collected and digitized and enable collation and correlation with UID and its partner databases
- Frame policies and administrative procedures related to hiring / retention / mobilization of resources, outsourcing of various tasks and budgeting & planning for UIDAI and all State units under UIDAI.

5. Planning Commission shall be the nodal agency for UIDAI for providing logistics, planning and budgetary support. Planning commission would provide initial office and IT infrastructure at central level.

Annexure 1

6. Government housing will be provided to officers of UIDAI appointed on deputation from general pool of Department of Urban Development.

(Dr. Subas Pani) 28/11/0
Secretary to the Government of India

The General Manager
Govt. of India Press
Faridabad.

Copy to:

1. Secretary to the President, Rashtrapati Bhavan, New Delhi
2. Secretary to the Vice-President, Maulana Azad Road, New Delhi
3. Cabinet Secretary, Rashtrapati Bhavan, New Delhi
4. Principal Secretary to the Prime Minister, South Block, New Delhi
5. Private Secretary to the Deputy Chairman, Planning Commission
6. All Ministers/Departments of Govt. of India
7. Chief Secretaries of all States/Union Territories
8. Secretary General, Rajya Sabha Secretariat, New Delhi
9. Secretary General, Lok Sabha Secretariat, New Delhi
10. Pr. Adviser (Admn & PC)/AS & FA/Adviser (C & I)/Director (GA)/DS (Admn.)
11. Pay & Accounts Officer, Planning Commission
12. Drawing & Disbursing Officer, Planning Commission
13. Accounts –I Section, Planning Commission.

4

TO BE INTRODUCED IN THE RAJYA SABHA

Bill No. LXXV of 2010

THE NATIONAL IDENTIFICATION AUTHORITY OF INDIA BILL, 2010

ARRANGEMENT OF CLAUSES

CHAPTER I

PRELIMINARY

CHAPTER II

AADHAAR NUMBERS

CHAPTER III

NATIONAL IDENTIFICATION AUTHORITY OF INDIA

CHAPTER IV

GRANTS, ACCOUNTS AND AUDIT AND ANNUAL REPORT

CHAPTER V

IDENTITY REVIEW COMMITTEE

CHAPTER VI

PROTECTION OF INFORMATION

CHAPTER VII

OFFENCES AND PENALTIES

CHAPTER VIII

MISCELLANEOUS

6

TO BE INTRODUCED IN THE RAJYA SABHA

Bill No. LXXV of 2010

THE NATIONAL IDENTIFICATION AUTHORITY OF INDIA BILL, 2010

A

BILL

to provide for the establishment of the National Identification Authority of India for the purpose of issuing identification numbers to individuals residing in India and to certain other classes of individuals and manner of authentication of such individuals to facilitate access to benefits and services to such individuals to which they are entitled and for matters connected therewith or incidental thereto.

BE it enacted by Parliament in the Sixty-first Year of the Republic of India as follows:—

CHAPTER I

PRELIMINARY

Short title, extent and commencement.

1. (*1*) This Act may be called the National Identification Authority of India Act, 2010.

(2) It shall extend to the whole of India except the State of Jammu and Kashmir and save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.

(*3*) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint; and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.

Definitions.

2. In this Act, unless the context otherwise requires,—

(*a*) "aadhaar number" means the identification number issued to an individual under sub-section (2) of section 3;

(*b*) "aadhaar number holder" means an individual who has been issued an aadhaar number under this Act;

(*c*) "authentication" means the process wherein, aadhaar number along with other attributes (including biometrics) are submitted to the Central Identities Data Repository for its verification and such Repository verifies the correctness thereof on the basis of information or data or documents available with it;

(*d*) "Authority" means the National Identification Authority of India established under sub-section (*1*) of section 11;

(*e*) "biometric information" means a set of such biological attributes of an individual as may be specified by regulations;

(*f*) "Central Identities Data Repository" means a centralised database in one or more locations containing all aadhaar numbers issued to aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto;

(*g*) "Chairperson" means the Chairperson of the Authority appointed under section 12;

(*h*) "demographic information" includes information relating to the name, age, gender and address of an individual (other than race, religion, caste, tribe, ethnicity, language, income or health), and such other information as may be specified in the regulations for the purpose of issuing an aadhaar number;

(*i*) "enrolling agency" means an agency appointed by the Authority or by the Registrars, as the case may be, for collecting information under this Act;

(*j*) "enrolment" means such process, as may be specified by regulations, to collect demographic information and biometric information from individuals by the enrolling agencies for the purpose of issuing of aadhaar number to such individuals under this Act;

(*k*) "identity information" in respect of an individual means biometric information, demographic information and aadhaar number of such individuals;

(*l*) "Member" includes the Chairperson and a part-time Member of the Authority appointed under section 12;

(*m*) "notification" means a notification published in the Official Gazette and the expression "notified" with its cognate meanings and grammatical variations shall be construed accordingly;

(*n*) "prescribed" means prescribed by rules made under this Act;

(*o*) "Registrar" means any entity authorised or recognised by the Authority for the purpose of enrolling the individuals under this Act;

(*p*) "regulations" means the regulations made by the Authority under this Act;

(*q*) "resident" means an individual usually residing in a village or rural area or town or ward or demarcated area (demarcated by the Registrar General of Citizen Registration) within a ward in a town or urban area in India;

(*r*) "Review Committee" means the Identification Review Committee constituted under sub-section (*1*) of section 28.

CHAPTER II

AADHAAR NUMBERS

Aadhaar number.

3. (*1*) Every resident shall be entitled to obtain an aadhaar number on providing of his demographic information and biometric information to the Authority in such manner as may be specified by regulations:

Provided that the Central Government may, from time to time, notify such other category of individuals who may be entitled to obtain an aadhaar number.

(2) On receipt of the demographic information and biometric information under sub-section (*1*), the Authority shall, after verifying the information, in such manner as may be specified by regulations, issue an aadhaar number to such resident.

Properties of aadhaar number.

4. (*1*) An aadhaar number, issued to an individual shall not be re-assigned to any other individual.

(2) An aadhaar number shall be a random number and bear no attributes or identity data or part thereof, relating to the aadhaar number holder.

(3) An aadhaar number shall, subject to authentication, be accepted as proof of identity of the aadhaar number holder.

Authentication of aadhaar number.

5. (*1*) The Authority shall perform authentication of the aadhaar number of a aadhaar number holder in relation to his biometric information and demographic information subject to such conditions and on payment of such fees and in such manner as may be specified by regulations.

(2) The Authority shall respond to an authentication query with a positive or negative response or with any other appropriate response excluding any demographic information and biometric information.

Aadhaar number not evidence of citizenship or domicile, etc.

6. The aadhaar number or the authentication thereof shall not, by itself, confer any right of or be proof of citizenship or domicile in respect of an aadhaar number holder.

Central Identities Data Repository.

7. The Authority may engage one or more entities to establish and maintain the Central Identities Data Repository and to perform any other functions as may be specified by regulations.

Updation of certain information.

8. The Authority may require the aadhaar number holders to update their demographic information and biometric information, from time to time, in such manner as may be specified by regulations so as to ensure continued accuracy of their information in the Central Identities Data Repository.

Prohibition on requiring certain information.

9. The Authority shall not require any individual to give information pertaining to his race, religion, caste, tribe, ethnicity, language, income or health.

Special measures for issuance of aadhaar number to certain categories of persons.

10. The Authority shall take special measures to issue aadhaar number to women, children, senior citizens, persons with disability, migrant unskilled and unorganised workers, nomadic tribes or to such other persons who do not have any permanent dwelling house and such other categories of individuals as may be specified by regulations.

CHAPTER III

NATIONAL IDENTIFICATION AUTHORITY OF INDIA

Establishment of Authority.

11. (*1*) The Central Government shall, by notification, establish an Authority to be known as the National Identification Authority of India to exercise the powers conferred on it and to perform the functions assigned to it under this Act.

(2) The Authority shall be a body corporate by the name aforesaid, having perpetual succession and a common seal, with power, subject to the provisions of this Act, to acquire, hold and dispose of property, both movable and immovable, and to contract, and shall, by the said name, sue or be sued.

(3) The head office of the Authority shall be in the National Capital Region referred to in clause (*f*) of section 2 of the National Capital Region Planning Board Act, 1985. 2 of 1985.

(4) The Authority may, with the prior approval of the Central Government, establish its offices at other places in India.

Composition of Authority.

12. The Authority shall consist of a Chairperson and two part-time Members to be appointed by the Central Government.

Qualifications for appointment of Chairperson and Members of Authority.

13. The Chairperson and Members of the Authority shall be persons of ability, integrity and outstanding calibre having experience and knowledge in the matters relating to technology, governance, law, development, economics, finance, management, public affairs or administration.

Term of office and other conditions of service of Chairperson and Members.

14. (*1*) The Chairperson and the Members appointed under this Act shall hold office for a term of three years from the date on which they assume office and shall be eligible for reappointment:

Provided that no person shall hold office as a Chairperson or Member after he has attained the age of sixty-five years:

Provided further that the Chairperson of the Unique Identification Authority of India appointed before the commencement of this Act by notification A-43011/02/2009-Admn.I (Vol.II) dated the 2nd July, 2009 shall continue as a Chairperson of the Authority under this Act for the term for which he had been appointed.

(2) The Chairperson and every Member shall, before entering upon their office, make and subscribe to, an oath of office and of secrecy, in such form and in such manner and before such Authority as may be prescribed.

(3) Notwithstanding anything contained in sub-section (*1*), the Chairperson or Member may—

(*a*) relinquish his office, by giving in writing to the Central Government, a notice of not less than thirty days; or

(*b*) be removed from his office in accordance with the provisions of section 15.

(4) The Chairperson shall not hold any other office during the period of holding his office in the Authority as such.

(5) The salaries and allowances payable to, and the other terms and conditions of service of, the Chairperson and allowances or remuneration payable to part-time Members shall be such as may be prescribed:

Provided that the salary, allowances and the other terms and conditions of service of the Chairperson shall not be varied to his disadvantage after his appointment.

Removal of Chairperson and Members.

15. (*1*) The Central Government may remove from office the Chairperson, or a Member, who—

(*a*) is, or at any time has been adjudged as an insolvent;

(*b*) has become physically or mentally incapable of acting as the Chairperson or, as the case may be, a Member;

(*c*) has been convicted of an offence which, in the opinion of the Central Government, involves moral turpitude;

(*d*) has acquired such financial or other interest as is likely to affect prejudicially his functions as the Chairperson or, as the case may be, a Member; or

(*e*) has, in the opinion of the Central Government, so abused his position as to render his continuance in office detrimental to the public interest.

(2) The Chairperson, or a Member shall not be removed under clause (*d*) or clause (*e*) of sub-section (*1*) unless he has been given a reasonable opportunity of being heard in the matter.

Restrictions on Chairperson or Members on employment after cessation of office.

16. The Chairperson or a Member, ceasing to hold office as such, shall not, without previous approval of the Central Government,—

(*a*) accept any employment in, or connected with the management or administration of, any person which has been associated with any work under the Act, for a period of three years from the date on which they cease to hold office:

Provided that nothing contained in this clause shall apply to any employment under the Central Government or a State Government or local authority or in any statutory authority or any corporation established by or under any Central, State or provincial Act or a Government Company, as defined in section 617 of the Companies Act, 1956;

1 of 1956.

(*b*) act, for or on behalf of any person or organisation in connection with any specific proceeding or transaction or negotiation or a case to which the Authority is a party and with respect to which the Chairperson or such Member had, before cessation of office, acted for or provided advice to, the Authority;

(*c*) give advice to any person using information which was obtained in his capacity as the Chairperson or a Member and being unavailable to or not being able to be made available to the public;

(*d*) enter, for a period of three years from his last day in office, into a contract of service with, accept an appointment to a board of directors of, or accept an offer of employment with, an entity with which he had direct and significant official dealings during his term of office as such.

Functions of Chairperson.

17. The Chairperson shall have powers of general superintendence, direction in the conduct of the affairs of the Authority and he shall, in addition to presiding over the meetings of the Authority, and without prejudice to any of the provisions of this Act, exercise and discharge such other powers and functions of the Authority as may be prescribed.

Meetings.

18. (*1*) The Authority shall meet at such times and places and shall observe such rules of procedure in regard to the transaction of business at its meetings (including quorum at such meetings) as may be specified by regulations.

(2) The Chairperson, or, if for any reason, he is unable to attend a meeting of the Authority, the senior most Member shall preside over the meetings of the Authority.

(*3*) All questions which come up before any meeting of the Authority shall be decided by a majority of votes by the Members present and voting and in the event of an equality of votes, the Chairperson or in his absence the Member presiding over shall have a second or casting vote.

(*4*) All decisions of the Authority shall be authenticated by the signature of the Chairperson or any other Member authorised by the Authority in this behalf.

(*5*) If any Member, who is a director of a company and who as such director, has any direct or indirect pecuniary interest in any matter coming up for consideration at a meeting of the Authority, he shall, as soon as possible after relevant circumstances have come to his knowledge, disclose the nature of his interest at such meeting and such disclosure shall be recorded in the proceedings of the Authority, and the Member shall not take part in any deliberation or decision of the Authority with respect to that matter.

Vacancies, etc., not to invalidate proceedings of Authority.

19. No act or proceeding of the Authority shall be invalid merely by reason of—

(*a*) any vacancy in, or any defect in the constitution of, the Authority;

(*b*) any defect in the appointment of a person as a Member of the Authority; or

(*c*) any irregularity in the procedure of the Authority not affecting the merits of the case.

Officers and other employees of Authority.

20. (*1*) There shall be a chief executive officer of the Authority, not below the rank of the Additional Secretary to the Government of India, who shall be the Member-Secretary of the Authority, to be appointed by the Central Government.

(*2*) The Authority may, with the approval of the Central Government, determine the number, nature and categories of other officers and employees required to the Authority in the discharge of its functions.

(*3*) **The salaries and allowances payable to, and the other terms and conditions of service of, the chief executive officer and other officers and other employees of the Authority shall be such as may be specified by regulations with the approval of the Central Government.**

Functions of chief executive officer of Authority.

21. (*1*) The chief executive officer shall be the legal representative of the Authority and shall be responsible for—

(*a*) the day-to-day administration of the Authority;

(*b*) implementing the work programmes and decisions adopted by the Authority;

(*c*) drawing up of proposal for the Authority's work programmes;

(*d*) the preparation of the statement of revenue and expenditure and the execution of the budget of the Authority.

(*2*) Every year, the chief executive officer shall submit to the Authority for approval—

(*a*) a general report covering all the activities of the Authority in the previous year;

(*b*) programmes of work;

(*c*) the annual accounts for the previous year; and

(*d*) the budget for the coming year.

(*3*) The chief executive officer shall have administrative control over the officers and other employees of the Authority.

Transfer of assets, liabilities of Authority.

22. On and from the establishment of the Authority —

(*1*) all the assets and liabilities of the Unique Identification Authority of India, established *vide* notification of the Government of India in the Planning Commission number A-43011/02/2009-Admin.I, dated the 28th January, 2009, shall stand transferred to, and vested in, the Authority.

Explanation.— The assets of such Unique Identification Authority of India shall be deemed to include all rights and powers, and all properties, whether movable or immovable, including, in particular, cash balances, deposits and all other interests and rights in, or arising out of, such properties as may be in the possession of such Unique Identification Authority of India and all books of account and other documents relating to the same; and liabilities shall be deemed to include all debts, liabilities and obligations of whatever kind;

(*2*) without prejudice to the provisions of sub-section (*1*), all data and information collected during enrolment, all details of authentication performed, debts, obligations and liabilities incurred, all contracts entered into and all matters and things engaged to be done by, with or for such Unique Identification Authority of India immediately before that day, for or in connection with the purpose of the said Unique Identification Authority of India, shall be deemed to have been incurred, entered into or engaged to be done by, with or for, the Authority;

(*3*) all sums of money due to the Unique Identification Authority of India immediately before that day shall be deemed to be due to the Authority; and

(*4*) all suits and other legal proceedings instituted or which could have been instituted by or against such Unique Identification Authority of India immediately before that day may be continued or may be instituted by or against the Authority.

Powers and functions of Authority.

23. (*1*) The Authority shall develop the policy, procedure and systems for issuing aadhaar numbers to residents and perform authentication thereof under this Act.

(*2*) Without prejudice to the provisions contained in sub-section (*1*), the powers and functions of the Authority may, *inter alia*, include all or any of the following matters, namely:—

(*a*) specifying, by regulation, demographic information and biometric information for enrolment for an aadhaar number and the processes for collection and verification thereof;

(*b*) collecting demographic information and biometric information from any individual seeking an aadhaar number in such manner as may be specified by regulations;

(*c*) appointing of one or more entities to operate the Central Identities Data Repository;

(*d*) generating and assigning aadhaar numbers to individuals;

(*e*) performing authentication of the aadhaar numbers;

(*f*) maintaining and updating the information of individuals in the Central Identities Data Repository in such manner as may be specified by regulations;

(*g*) omitting and deactivating of an aadhaar number and information relating thereto in such manner as may be specified by regulations;

(*h*) specify the usage and applicability of the aadhaar number for delivery of various benefits and services as may be provided by regulations;

(*i*) specifying, by regulation, the terms and conditions for appointment of Registrars, enrolling agencies and service providers and revocation of appointments thereof;

(*j*) establishing, operating and maintaining of the Central Identities Data Repository;

(*k*) sharing, in such manner as may be specified by regulations, the information of aadhaar number holders, with their written consent, with such agencies engaged in delivery of public benefits and public services as the Authority may by order direct;

(*l*) calling for information and records, conducting inspections, inquiries and audit of the operations for the purposes of this Act of the Central Identities Data Repository, Registrars, enrolling agencies and other agencies appointed under this Act;

(*m*) specifying, by regulation, various processes relating to data management, security protocols and other technology safeguards under this Act;

(*n*) specifying, by regulation, the conditions and procedures for issuance of new aadhaar number to existing aadhaar number holder;

(*o*) levy and collect the fees or authorise the Registrars, enrolling agencies or other service providers to collect such fees for the services provided by them under this Act in such manner as may be specified by regulations;

(*p*) appoint such committees as may be necessary to assist the Authority in discharge of its functions for the purposes of this Act;

(*q*) promote research and development for advancement in biometrics and related areas, including usage and applications of aadhaar numbers through appropriate mechanisms;

(*r*) specifying, by regulation, the policies and practices for Registrars, enrolling agencies and other service providers;

(*s*) setting up facilitation centres and grievance redressal mechanisms for redressal of grievances of residents, Registrars, enrolling agencies and other service providers;

(*t*) such other powers and functions as may be prescribed.

(*3*) The Authority may,—

(*a*) enter into a Memorandum of Understanding or agreement, as the case may be, with Central Government or State Governments or Union territories or other agencies for the purpose of performing any of the functions in relation to collecting, storing, securing or processing of information or performing authentication;

(*b*) by notification, appoint such number of Registrars, engage and authorise such agencies to collect, store, secure, process information or do authentication or perform such other functions in relation thereto,

as may be necessary for the purposes of this Act.

(*4*) The Authority may engage such consultants, advisors and other persons as may be required for efficient discharge of its functions under this Act on such allowances or remuneration and terms and conditions as may be specified by regulations.

CHAPTER IV

GRANTS, ACCOUNTS AND AUDIT AND ANNUAL REPORT

Grants by Central Government.

24. The Central Government may, after due appropriation made by Parliament by law in this behalf, make to the Authority, grants of such sums of money as the Central Government may think fit for being utilised for the purposes of this Act.

Other fees and revenue.

25. The fees or revenue collected by the Authority shall be credited to the Consolidated Fund of India and the entire amount so credited be transferred to the Authority.

Accounts and audit.

26. (*1*) The Authority shall maintain proper accounts and other relevant records and prepare an annual statement of accounts in such form as may be prescribed by the Central Government in consultation with the Comptroller and Auditor-General of India.

(*2*) The accounts of the Authority shall be audited annually by the Comptroller and Auditor-General of India at such intervals as may be specified by him and any expenditure incurred in connection with such audit shall be payable by the Authority to the Comptroller and Auditor-General.

(*3*) The Comptroller and Auditor-General and any person appointed by him in connection with the audit of the accounts of the Authority under this Act shall have the same rights and privileges and authority in connection with such audit as the Comptroller and Auditor-General generally has in connection with the audit of Government accounts, and in particular, shall have the right to demand production of books, accounts, connected vouchers and other documents and papers, and to inspect any of the offices of the Authority.

(*4*) The accounts of the Authority, as certified by the Comptroller and Auditor-General or any other person appointed by him in this behalf, together with the audit report thereon shall be forwarded annually to the Central Government by the Authority and the Central Government shall cause the audit report to be laid, as soon as may be after it is received, before each House of Parliament.

Returns and annual report, etc.

27. (*1*) The Authority shall furnish to the Central Government at such time and in such form and manner as may be prescribed or as the Central Government may direct, such returns and statements and particulars in regard to any matter under the jurisdiction of the Authority, as the Central Government may from time to time require.

(*2*) The Authority shall prepare, once in every year, and in such form and manner and at such time as may be prescribed, an annual report giving—

(*a*) a description of all the activities of the Authority for the previous years;

(*b*) the annual accounts for the previous year; and

(*c*) the programmes of work for coming year.

(*3*) A copy of the report received under sub-section (*2*) shall be laid by the Central Government, as soon as may be after it is received, before each House of Parliament.

CHAPTER V

IDENTITY REVIEW COMMITTEE

Review Committee.

28. (*1*) The Central Government may, by notification, constitute the Identity Review Committee to discharge functions specified under sub-section (*1*) of section 29 in respect of any matter connected with the usage of the aadhaar numbers.

(*2*) The Review Committee shall consist of three members (one of whom shall be chairperson designated as such by the Central Government) who are persons of eminence, ability, integrity and standing in public life having knowledge and experience in the fields of technology, law, administration and governance, social service, journalism, management or social sciences.

(*3*) The members of the Review Committee shall be appointed by the Central Government on the recommendations of a committee consisting of—

(*a*) the Prime Minister, who shall be the Chairperson of the committee;

(*b*) the Leader of Opposition in the Lok Sabha; and

(*c*) a Union Cabinet Minister to be nominated by the Prime Minister.

Explanation.— For the removal of doubts, it is hereby declared that where the Leader of the Opposition in the House of the People has not been recognised as such, the Leader of the single largest group in Opposition of the Government in the House of the People shall be deemed to be the Leader of the Opposition.

(*4*) The member of the Review Committee shall not be a Member of Parliament or Member of the Legislature of any State or Union territory, as the case may be, or a member of any political party.

(*5*) The members of the Review Committee shall hold office for a term of three years from the date on which they enter upon office and shall not be eligible for reappointment.

(*6*) The Central Government may by order remove from office any member of the Review Committee, who—

(*a*) is, or at any time has been adjudged as an insolvent;

(*b*) has become physically or mentally incapable of acting as a member;

(*c*) has been convicted of an offence which, in the opinion of the Central Government, involves moral turpitude;

(*d*) has acquired such financial or other interest as is likely to affect prejudicially his functions as a member; or

(*e*) has, in the opinion of the Central Government, so abused his position as to render his continuance in office detrimental to the public interest:

Provided that a Member shall not be removed under clause (*d*) or clause (*e*) unless he has been given a reasonable opportunity of being heard in the matter.

Functions of Review Committee.

29. (*1*) The Review Committee shall ascertain the extent and pattern of usage of the aadhaar numbers across the country and prepare a report annually in relation to the extent and pattern of usage of the aadhaar numbers along with its recommendations thereon and submit the same to the Central Government.

(*2*) The manner of preparation of the report referred to in sub-section (*1*) shall be such as may be determined by the Review Committee.

(*3*) A copy of the report along with the recommendations of the Review Committee shall be laid by the Central Government, as soon as may be after it is received, before each House of Parliament.

CHAPTER VI

PROTECTION OF INFORMATION

Security and confidentiality of information.

30. (*1*) The Authority shall ensure the security and confidentiality of identity information and authentication records of individuals.

(*2*) The Authority shall take measures (including security safeguards) to ensure that the information in the possession or control of the Authority (including information stored in the Central Identities Data Repository) is secured and protected against any loss or unauthorised access or use or unauthorised disclosure thereof.

(*3*) Notwithstanding anything contained in any other law and save as otherwise provided in this Act, the Authority or any of its officer or other employee or any agency who maintains the Central Identities Data Repository shall not, whether during his service as such or thereafter, reveal any information stored in the Central Identities Data Repository to any person:

Provided that an aadhaar number holder may request the Authority to provide access to his identity information in such manner as may be specified by regulations.

Alteration of demographic information or biometric information.

31. (*1*) In case any demographic information relating to an aadhaar number holder is found incorrect or changes subsequently, the aadhaar number holder shall request the Authority to alter such demographic information in his record in the Central Identities Data Repository in such manner as may be specified by regulations.

(*2*) In case any biometric information of aadhaar number holder is lost or changes subsequently for any reason, the aadhaar number holder shall request the Authority to make necessary alteration in his record in the Central Identities Data Repository in such manner as may be specified by regulations.

(*3*) On receipt of any request under sub-section (*1*) or sub-section (*2*), the Authority may, if it is satisfied, make such alteration as may be required in the record relating to such aadhaar number holder and intimate such alteration to the concerned aadhaar number holder.

Access to own information and records of requests for authentication.

32. (*1*) The Authority shall maintain details of every request for authentication of the identity of every aadhaar number holder and the response provided thereon by it in such manner and for such time as may be specified by regulations.

(*2*) Every aadhaar number holder shall be entitled to obtain details of request for authentication of his aadhaar number and the response provided thereon by the Authority in such manner as may be specified by regulations.

Disclosure of information in certain cases.

33. Nothing contained in sub-section (*3*) of section 30 shall apply in respect of—

(*a*) any disclosure of information (including identity information or details of authentication) made pursuant to an order of a competent court; or

(*b*) any disclosure of information (including identity information) made in the interests of national security in pursuance of a direction to that effect issued by an officer or officers not below the rank of Joint Secretary or equivalent in the Central Government specifically authorised in this behalf by an order of the Central Government.

CHAPTER VII

OFFENCES AND PENALTIES

Penalty for impersonation at time of enrolment.

34. Whoever impersonates or attempts to impersonate another person, whether dead or alive, real or imaginary, by providing any false demographic information or biometric information shall be punishable with imprisonment for a term which may extend to three years and with a fine which may extend to ten thousand rupees.

Penalty for impersonation of aadhaar number holder by changing demographic information or biometric information.

35. Whoever, with the intention of causing harm or mischief to a aadhaar number holder, or with the intention of appropriating the identity of a aadhaar number holder changes or attempts to change any demographic information or biometric information of a aadhaar number holder by impersonating or attempting to impersonate another person, dead or alive, real or imaginary, shall be punishable with imprisonment for a term which may extend to three years and shall be liable to a fine which may extend to ten thousand rupees.

Penalty for impersonation.

36. Whoever, not being authorised to collect identity information under the provisions of this Act, by words, conduct or demeanour pretends that he is authorised to do so, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

Penalty for disclosing identity information.

37. Whoever, intentionally discloses, transmits, copies or otherwise disseminates any identity information collected in the course of enrolment or authentication to any person not authorised under this Act shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

Penalty for unauthorised access to the Central Identities Data Repository.

38. Whoever, not being authorised by the Authority, intentionally,—

(*a*) accesses or secures access to the Central Identities Data Repository; or

(*b*) downloads, copies or extracts any data from the Central Identities Data Repository or stored in any removable storage medium; or

(*c*) introduces or causes to be introduced any virus or other computer contaminant in the Central Identities Data Repository; or

(*d*) damages or causes to be damaged the data in the Central Identities Data Repository; or

(*e*) disrupts or causes disruption of the access to the Central Identities Data Repository; or

(*f*) denies or causes a denial of access to any person who is authorised to access the Central Identities Data Repository; or

(*g*) provides any assistance to any person to do any of the acts aforementioned; or

(*h*) destroys, deletes or alters any information stored in any removable storage media or in the Central Identities Data Repository or diminishes its value or utility or effects it injuriously by any means; or

(*i*) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used by the Authority with an intention to cause damage,

shall be punishable with imprisonment for a term which may extend to three years and shall be liable to a fine which shall not be less than one crore rupees.

Explanation.— For the purposes of this section, the expressions "computer contaminant", "computer virus" and "damage" shall have the meanings respectively assigned to them in the *Explanation* to section 43 of the Information Technology Act, 2000. 21 of 2000.

Penalty for tampering with data in Central Identities Data Repository.

39. Whoever, not being authorised by the Authority, uses or tampers with the data in the Central Identities Data Repository or in any removable storage medium with the intent of modifying information relating to aadhaar number holder or discovering any information thereof shall be punishable with imprisonment for a term which may extend to three years and shall be liable to a fine which may extend to ten thousand rupees.

Penalty for manipulating biometric information.

40. Whoever gives or attempts to give any biometric information which does not pertain to him for the purpose of getting an aadhaar number or authentication or updating his information, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or with both.

General penalty.

41. Whoever, commits an offence under this Act for which no penalty is provided elsewhere than in this section, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to twenty-five thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

Offences by companies.

42. (*1*) Where an offence under this Act has been committed by a company, every person who at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to any punishment provided in this Act if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence.

(2) Notwithstanding anything contained in sub-section (*1*), where any offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to, any neglect on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

Explanation.— For the purposes of this section—

(*a*) "company" means any body corporate and includes a firm or other association of individuals; and

(*b*) "director", in relation to a firm, means a partner in the firm.

Act to apply for offence or contravention committed outside India.

43. (*1*) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person, irrespective of his nationality.

(2) For the purposes of sub-section (*1*), the provisions of this Act shall apply to any offence or contravention committed outside India by any person, if the act or conduct constituting the offence or contravention involves the Central Identities Data Repository.

Power to investigate offences.

44. Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector of Police shall investigate any offence under this Act. 2 of 1974.

Penalties not to interfere with other punishments.

45. No penalty imposed under this Act shall prevent the imposition of any other penalty or punishment under any other law for the time being in force.

Cognizance of offences.

46. (*1*) No court shall take cognizance of any offence punishable under this Act, save on a complaint made by the Authority or any officer or person authorised by it.

(2) No court inferior to that of a Chief Metropolitan Magistrate or a Chief Judicial Magistrate shall try any offence punishable under this Act.

CHAPTER VIII

MISCELLANEOUS

Power of Central Government to supersede Authority.

47. (*1*) If, at any time, the Central Government is of the opinion,—

(*a*) that, on account of circumstances beyond the control of the Authority, it is unable to discharge the functions or perform the duties imposed on it by or under the provisions of this Act; or

(*b*) that the Authority has persistently defaulted in complying with any direction given by the Central Government under this Act or in the discharge of the functions or performance of the duties imposed on it by or under the provisions of this Act and as a result of such default the financial position of the Authority or the administration of the Authority has suffered; or

(*c*) that circumstances exist which render it necessary in the public interest so to do,

the Central Government may, by notification, supersede the Authority for such period, not exceeding six months, as may be specified in the notification and appoint a person or persons as the President may direct to exercise powers and discharge functions under this Act:

Provided that before issuing any such notification, the Central Government shall give a reasonable opportunity to the Authority to make representations against the proposed supersession and shall consider the representations, if any, of the Authority.

(*2*) Upon the publication of a notification under sub-section (*1*) superseding the Authority,—

(*a*) the Chairperson and other members shall, as from the date of supersession, vacate their offices as such;

(*b*) all the powers, functions and duties which may, by or under the provisions of this Act, be exercised or discharged by or on behalf of the Authority shall, until the Authority is reconstituted under sub-section (*3*), be exercised and discharged by the person or persons referred to in sub-section (*1*); and

(*c*) all properties owned or controlled by the Authority shall, until the Authority is reconstituted under sub-section (*3*), vest in the Central Government.

(*3*) On or before the expiration of the period of supersession specified in the notification issued under sub-section (*1*), the Central Government shall reconstitute the Authority by a fresh appointment of its Chairperson and other members and in such case any person who had vacated his office under clause (*a*) of sub-section (*2*) shall not be deemed to be disqualified for reappointment.

(*4*) The Central Government shall cause a copy of the notification issued under sub-section (*1*) and a full report of any action taken under this section and the circumstances leading to such action to be laid before each House of Parliament at the earliest.

Members, officers, etc., to be public servants.

48. The Chairperson, Members, officers and other employees of the Authority shall be deemed, while acting or purporting to act in pursuance of any of the provisions of this Act, to be public servants within the meaning of section 21 of the Indian Penal Code. 45 of 1860.

Power of Central Government to issue directions.

49. Without prejudice to the foregoing provisions of this Act, the Authority shall, in exercise of its powers or the performance of its functions under this Act be bound by such directions on questions of policy, other than those relating to technical and administrative matters, as the Central Government may give, in writing to it, from time to time:

Provided that the Authority shall, as far as practicable, be given an opportunity to express its views before any direction is given under this sub-section.

(*2*) The decision of the Central Government, whether a question is one of policy or not, shall be final.

Delegation.

50. The Authority may, by general or special order in writing, delegate to any Member, officer of the Authority or any other person, subject to such conditions, if any, as may be specified in the order, such of its powers and functions under this Act (except the power under section 53) as it may deem necessary.

Protection of action taken in good faith.

51. No suit, prosecution or other legal proceeding shall lie against the Central Government or the Authority or the Chairperson or any Member or any officer, or other employees of the Authority for anything which is in good faith done or intended to be done under this Act or the rule or regulation made thereunder.

Power of Central Government to make rules.

52. (*1*) The Central Government may, by notification, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:—

(*a*) the form and manner in which and the Authority before whom the oath of office and of secrecy is to be subscribed by the Chairperson and Members under sub-section (2) of section 14;

(*b*) the salary and allowances payable to, and other terms and conditions of service of, the Chairperson and the allowances or remuneration payable to Members of the Authority under sub-section (*5*) of section 14;

(*c*) the other powers and functions of the Chairperson of the Authority under section 17;

(*d*) the other powers and functions of the Authority under clause (*t*) of sub-section (2) of section 23;

(*e*) the form of annual statement of accounts to be prepared by the Authority under sub-section (*1*) of section 26;

(*f*) the form and the manner in which and the time within which returns and statements and particulars are to be furnished under sub-section (*1*) of section 27;

(*g*) the form and the manner and the time at which the Authority shall furnish annual report under sub-section (2) of section 27;

(*h*) any other matter which is required to be, or may be, prescribed, or in respect of which provision is to be or may be made by rules.

Power of Authority to make regulations.

53. (*1*) The Authority may, by notification, make regulations consistent with this Act and the rules made thereunder, for carrying out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely:—

(*a*) the biometric information under clause (*c*) and the demographic information under clause (*h*) of section 2;

(*b*) the process of collecting demographic information and biometric information from the individuals by enrolling agencies under clause (*j*) of section 2;

(*c*) the manner of furnishing the demographic information and biometric information by the resident under sub-section (*1*) of section 3;

(*d*) the manner of verifying the demographic information and biometric information for issue of aadhaar number under sub-section (*2*) of section 3;

(*e*) the conditions, fees and manner of authentication of the aadhaar number under sub-section (*1*) of section 5;

(*f*) the other functions to be performed by Central Identities Data Repository under section 7;

(*g*) the manner of updating biometric information and demographic information under section 8;

(*h*) the other categories of individuals under section 10 for whom the Authority shall take special measures for issue of aadhaar number;

(*i*) the time and places of meetings of the Authority and the procedure for transaction of business to be followed by it (including the quorum) under sub-section (*1*) of section 18;

(*j*) the salary and allowances payable to, and other terms and conditions of service of, the chief executive officer, officers and other employees of the Authority under sub-section (*3*) of section 20;

(*k*) the demographic information and biometric information and process for their collection and verification under clause (*a*) and the manner of their collection under clause (*b*) of sub-section (*2*) of section 23;

(*l*) the manner of maintaining and updating the information of individuals in the Central Identities Data Repository under clause (*f*) of sub-section (*2*) of section 23;

(*m*) the manner of omitting and deactivating an aadhaar number and information relating thereto under clause (*g*) of sub-section (*2*) of section 23;

(*n*) the usage and applicability of the aadhaar number for delivery of various benefits and services under clause (*h*) of sub-section (*2*) of section 23;

(*o*) the terms and conditions for appointment of Registrars, enrolling agencies and other service providers and the revocation of appointments thereof under clause (*i*) of sub-section (*2*) of section 23;

(*p*) the manner of sharing information of aadhaar number holder under clause (*k*) of sub-section (*2*) of section 23;

(*q*) various processes relating to data management, security protocol and other technology safeguards under clause (*m*) of sub-section (*2*) of section 23;

(*r*) the procedure for issuance of new aadhaar number to existing aadhaar number holder under clause (*n*) of sub-section (*2*) of section 23;

(*s*) manner of authorising Registrars, enrolling agencies or other services providers to collect such fees for services provided by them under clause (*o*) of sub-section (*2*) of section 23;

(*t*) policies and practices to be followed by the Registrar, enrolling agencies and other service providers under clause (*r*) of sub-section (*2*) of section 23;

(*u*) the allowances or remuneration and terms and conditions of consultants, advisors and other persons under sub-section (*4*) of section 23;

(*v*) the manner in which an aadhaar number holder can access his identity information under sub-section (*3*) of section 30;

(*w*) the manner of alteration of demographic information under sub-section (*1*) and biometric information under sub-section (*2*) of section 31;

(*x*) the manner of and the time for maintaining the details of request for authentication and the response thereon under sub-section (*1*) of section 32;

(*y*) the manner of obtaining, by the aadhaar number holder, the records of request for authentication of his aadhaar number and response thereon under sub-section (*2*) of section 32;

(*z*) any other matter which is required to be, or may be, specified, or in respect of which provision is to be or may be made by regulations.

Laying of rules and regulations before Parliament.

54. Every rule and every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or regulation, or both Houses agree that the rule or regulation should not be made, the rule or regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule or regulation.

Application of other laws not barred.

55. The provisions of this Act shall be in addition to, and not in derogation of, any other law for the time being in force.

Power to remove difficulties.

56. (*1*) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order, published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to be necessary for removing the difficulty:

Provided that no such order shall be made under this section after the expiry of two years from the commencement of this Act.

(2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

Savings.

57. Anything done or any action taken by the Central Government under the Resolution of the Government of India, Planning Commission bearing notification number A-43011/02/2009-Admin.I, dated the 28th January, 2009, shall be deemed to have been done or taken under the corresponding provisions of this Act.

STATEMENT OF OBJECTS AND REASONS

The Central Government had decided to issue unique identification numbers to all residents in India and to certain other persons. The scheme of unique identification involves collection of demographic information and biometric information from individuals for the purpose of issuing of unique identification numbers to such individuals. The biometric information would involve taking of a set of biological attributes of such individuals.

2. The Central Government, for the purposes of issue of the unique identification numbers, constituted, *vide* its notification dated the 28th January, 2009 being of executive in nature, the Unique Identification Authority of India, which is at present functioning under the Planning Commission.

3. It has been observed and assessed that the issue of unique identification numbers may involve certain issues, such as (a) security and confidentiality of information, imposition of obligation of disclosure of information so collected in certain cases, (b) impersonation by certain individuals at the time of enrolment for issue of unique identification numbers, (c) unauthorised access to the Central Identities Data Repository, (d) manipulation of biometric information, (e) investigation of certain acts constituting offence, and (f) unauthorised disclosure of the information collected for the purposes of issue of the unique identification numbers which should be addressed by law and attract penalties.

4. In view of the foregoing paragraph, it has been felt necessary to make the said Authority as a statutory authority for carrying out the functions of issuing identification numbers to the residents in India in an effective manner. It is, therefore, proposed to enact the National Identification Authority of India Bill, 2010 to provide for the establishment of the National Identification Authority of India for the prupose of issuing identification numbers (which has been referred to as aadhaar number) to individuals residing in India and to certain other classes of individuals and manner of authentication of such individuals to facilitate access to benefits and services to such individuals to which they are entitled and for matters connected therewith or incidental thereto.

5. The National Identification Authority of India Bill, 2010, *inter alia*, seeks to provide—

(*a*) for issue of aadhaar numbers to every resident by the Authority on providing his demographic information and biometric information to it in such manner as may be specified by regulations;

(*b*) for authentication of the aadhaar number of an aadhaar number holder in relation to his biometric information and demographic information subject to such conditions and on payment of such fees as may be specified by regulations;

(*c*) for establishment of the National Identification Authority of India consisting of a Chairperson and two part-time Members;

(*d*) that the Authority to exercise powers and discharge functions which, *inter alia*, include—

(*i*) specifying the demographic information and biometric information for enrolment for an aadhaar number and the processes for collection and verification thereof;

(*ii*) collecting demographic information and biometric information from any individual seeking an aadhaar number in such manner as may be specified by regulations;

(*iii*) appointing of one or more entities to operate the Central Identities Data Repository;

(*iv*) maintaining and updating the information of individuals in the Central Identities Data Repository in such manner as may be specified by regulations;

(*v*) specify the usage and applicability of the aadhaar number for delivery of various benefits and services as may be provided by regulations;

(*e*) that the Authority shall not require any individual to give information pertaining to his race, religion, caste, tribe, ethnicity, language, income or health;

(*f*) that the Authority may engage one or more entities to establish and maintain the Central Identities Data Repository and to perform any other functions as may be specified by regulations;

(*g*) for constitution of the Identity Review Committee consisting of three members (one of whom shall be the chairperson) to ascertain the extent and pattern of usage of the aadhaar numbers across the country and prepare a report annually in relation to the extent and pattern of usage of the aadhaar numbers along with its recommendations thereon and submit the same to the Central Government;

(*h*) that the Authority shall take measures (including security safeguards) to ensure that the information in the possession or control of the Authority (including information stored in the Central Identities Data Repository) is secured and protected against any loss or unauthorised access or use or unauthorised disclosure thereof;

(*i*) for offences and penalties for contravention of the provisions of the proposed legislation.

6. The notes on clauses explain in detail the various provisions contained in the Bill.

7. The Bill seeks to achieve the above objectives.

NEW DELHI:
The 8th November, 2010.

MANMOHAN SINGH

24

UIDAI - FAQs

Protection from Expanding Data Fields

How will the UIDAI protect against functional creep?

The full board of UIDAI may add additional data fields related to identity, and the law will contain a prescription against collecting any other information besides the information permitted, with specific prohibitions against collection of information regarding religion, race, ethnicity, caste and other similar matters and the facilitation of analysis of the data for anyone or to engage in profiling or any similar activity.

Children

How will children be captured in the database?

For children below 5 years no biometrics will be captured. Their UID be processed on the basis of demographic information and facial photograph linked with the UID of their parents. These children will need to be re-enrolled with biometrics of ten fingers, iris and facial photograph, when they turn 5. Their biometrics will be updated once they turn 15. Intimation to this effect will be mentioned in the original Aadhaar letter.

Differently-abled

How will the biometric of the differently-abled and people with no finger prints or rugged hands e.g. beedi workers or people with no fingers be captured?

The policy will take into consideration these exceptions and the biometric standards prescribed will ensure that these groups are not excluded. In the case of people without hands/ fingers only photo will be used for identity determination and there will be markers to determine uniqueness.

Language & Transliteration

How do I enter data in local language?

A local language can be selected during the setup of the enrolment client. The list of available options is a subset of the Input Method Editors (IMEs) installed on the enrolment station. For instance, the operator can install the Google IME (or an IME available from a different source) for Hindi input. When the data entry is performed in English, the text is also transliterated through the IME, and placed on the screen. The operator can then correct this text, using the IME's built in editing tools, including a virtual keyboard. Certain IMEs allow users to specify a set of macros, and other smart tools to allow easier data entry in the local language.

What do you mean when you say that a particular language is supported?

Supporting a local language implies providing support for:
Data entry in local language
Transliteration of English language data to local language
Labels in local language in the software (on screen)
Labels in local language in the print receipt
Import of pre-enrolment data in local language (upcoming)

What languages are supported?

In the current release (1.2.1.5), we have support for
Hindi
Kannada
Telugu
Tamil
Marathi
Bengali

In future releases, subject to availability of a local language IME, we expect to support additional Indian languages

How do I make local language the primary source for data entry?

At this time, the primary source for data entry is in English. However, as the technology matures, we expect to change the primary language to local language based on reverse transliteration. Since this is a dependency on technology that is not yet available, we cannot assure a date, however – we are targeting a release in Version 3.0.

What are the common issues seen with Indian Language Input?

The most common problem that UIDAI have seen is with installation of the IME, and it's interactions with the language bar. Further, it is possible to configure the Windows language input to assume a local language keyboard. This is not the same as transliteration, but assumes a different keyboard is being used – and the results are very different. UIDAI have also had difficulty in truly transliterating English words into local language, as they are very different from the language model. This can be better handled by using advanced facilities in the IMEs (for ex. Schemes in Google IME) The language support must be configured on a per user basis, and that makes it harder to manage.

How do I import pre-enrolment data in local language?

At this time, the support has been provided for import of pre-enrolment data in English. During enrolment process, the data is converted from English to local language through the transliteration engine. The operator can correct this data in the presence of the resident. The software is planned to provide support for import of pre-enrolment data in English, local language or both in future versions. For pre-enrolment data imported in local language, it will

not be over-ridden by the transliteration engine. However, a soft keypad / IME will be available for editing the data.

What language will the database be maintained? In what language will authentication services be provided? In what language will communication between UIDAI and the resident take place?

The database will be maintained in English. The communication between resident and UIDAI will be in English and the local language.

Protection of Individual information in UIDAI system

What are the privacy protections in place to protect the right to privacy of the resident?

Protection of the individual and the safeguarding their information is inherent in the design of the UID project. From having a random number which does not reveal anything about the individual to other features listed below, the UID project keeps the interest of the resident at the core of its purpose and objectives.

- **Collecting limited information**

The UIDAI is collecting only basic data fields - Name, Date of Birth, Gender, Address, Parent/ Guardian's (name essential for children but not for others) photo, 10 finger prints and iris scan.

- **No profiling and tracking information collected**

The UIDAI policy bars it from collecting sensitive personal information such as religion, caste, community, class, ethnicity, income and health. The profiling of individuals is therefore not possible through the UID system.

- **Release of information – yes or no response**

The UIDAI will not reveal personal information in the Aadhaar database – the only response will be a 'yes' or 'no' to requests to verify an identity

- **Convergence and linking of UIDAI information to other databases**

The UID database is not linked to any other databases, or to information held in other databases. Its only purpose will be to verify a person's identity at the point of receiving a

service, and that too with the consent of the aadhaar number holder.
The UID database will be guarded both physically and electronically by a few select individuals with high clearance. The data will be secured with the best encryption, and in a highly secure data vault. All access details will be properly logged.

What are the Data protection and privacy measures taken by UIDAI ?

The UIDAI has the obligation to ensure the security and confidentiality of the data collected. The data will be collected on software provided by the UIDAI and encrypted to prevent leaks in transit. The UIDAI has a comprehensive security policy to ensure the safety and integrity of its data. There are security and storage protocols in place. UIDAI has published guidelines in this regard which is available on its website.
Penalties for any security violation will be severe, and include penalties for disclosing identity information. There will also be penal consequences for unauthorised access to CIDR – including hacking, and penalties for tampering with data in the CIDR.

What are the possible criminal penalties envisaged against the fraud or unauthorized access to data. ?

Following are the possible criminal penalties in the Bill:
• Impersonation by providing false demographic or biometric information is an offence – imprisonment for 3 years and a of fine Rs. 10,000.
• Appropriating the identity of an Aadhaar number holder by changing or attempting to change the demographic and biometric information of an Aadhaar number holder is an offence - imprisonment for 3 years and a fine of Rs. 10,000.
• Pretending to be an agency authorized to collect Identity information of a resident is an offence – imprisonment for 3 years and a fine of Rs. 10,000 for a person, and Rs. 1 lakh for a company.
• Intentionally transmitting information collected during enrolment and authentication to an unauthorized person is an offence – imprisonment for 3 years and a fine of Rs. 10,000 for a person, and Rs. 1lakh for a company.
• Unauthorized access to the central identities data repository (CIDR) and hacking is an offence – imprisonment for 3 years and a fine of Rs. 1 crore.
• Tampering with the central identities data repository is an offence – imprisonment for 3 years and a fine of Rs. 10,000.
• Providing biometrics that is not one's own is an offence – imprisonment for 3 years and of Rs. 10,000.

Grievance Redressal Mechanism

Will there be a grievance redressal mechanism?

Yes, there will be concern and issues that residents or UIDAI eco system partner may have in terms of enrolment, authentication and identity frauds etc. . The UIDAI has set up a Contact Centre that serves as a single point of contact for the organization. The existing channels of communications are :
Voice (Helpline number: 1800 3001947), FAX (080-2353 1947 ,Letter (P.O. Box number 1947, Bengaluru- 560 001) and E-mail (help@uidai.gov.in).

What is the Registrar / EA's role in grievance resolution?

The registrar is expected to put in place a team that would serve to quickly address any matters requiring resolution that may pertain to the Registrar, but may be conveyed to the UIDAI Contact Centre. Queries / grievances which need Registrar/enrolment agency involvement will be transferred to the Registrar appointed nodal officer through a web portal. The time taken for resolutions will be finalized jointly.

What if a Resident gets rejected by the UIDAI and is not issued the Aadhaar no.?

The reason for rejection along with steps to be taken post rejection will be communicated to the resident and the Registrar.

What if a Resident misplaces his Aadhaar letter /forgets his Aadhaar no.?

The resident can contact the Contact Centre (through phone / letter / email) with the enrolment number and make a request for sending a second letter communicating the Aadhaar number. This may be a paid service.
In case the Aadhaar number has been used to avail a service or benefit, the resident can contact the agency that offers the same, to obtain the Aadhaar number.

What if the Aadhaar letter does not get delivered to a Resident?

Your Aadhaar number should reach the address provided during enrolment normally within 90 days of enrolment. If not, the resident will need to call/email the UIDAI Contact Centre with the enrolment number.

What can the Resident do if there are spelling mistakes / other demographic error in his/her Aadhaar letter?

During enrolment, even when the data is entered, the resident can see the data entry and is expected to point out errors at this stage. Prior to finalization and printing of the Enrolment Acknowledgment, one more opportunity is presented to make corrections.

In the event that both opportunities are missed, the demographic correction may be carried out by visiting the enrolment centre within 48 hours of time of enrolment carrying the relevant documents and enrolment slip.

Financial Inclusion

What can the Resident do if there are spelling mistakes / other demographic error in his/her Aadhaar letter?

During enrolment, even when the data is entered, the resident can see the data entry and is expected to point out errors at this stage. Prior to finalization and printing of the Enrolment Acknowledgment, one more opportunity is presented to make corrections.

In the event that both opportunities are missed, the demographic correction may be carried out by visiting the enrolment centre within 48 hours of time of enrolment carrying the relevant documents and enrolment slip.

What is the pre-requisite to initiate payment through APB?

There are three primary requirements before a payment can be made successfully using APB:

- The Resident's Aadhaar to be linked with the Bank Account;
- Aadhaar to be linked in the database of the paying agency, such as a Government Welfare Scheme;
- The Paying agency to be registered on APB and get an APB Registration ID.

What is AePS?

AePS (Aadhaar Enabled Payments System) is a payment service offered by the National Payments Corporation of India (NPCI) to banks, financial institutions using 'Aadhaar' number and online UIDAI authentication through their respective Business correspondent service Centers / Bank Mitras.

Does the Resident need to have a bank account for availing AEPS?

Yes, the customer needs to have a bank account linked to his/ her Aadhaar with the bank offering the AEPS service.

What is Aadhaar Seeding?

Aadhaar Seeding is the process of linking the Aadhaar in various beneficiary databases. Examples include linking of Aadhaar to the Bank Accounts, to Pension ID for Pensioners and to Job Card Number of NREGS Wage Seekers, etc.

Can a Resident link the Aadhaar to more than one account within a bank?

Yes. However the bank shall keep only one of the accounts as primary account which would receive all AEPS transactions.

Can a Resident link the Aadhaar to more than one Account in different Banks?

Yes. However, the Account that has been Seeded last backed with a mandate to the bank to receive payments – will be active for receiving payments through APB.

What is the e-KYC service?

UIDAI offers the e-KYC service, which enables a resident having an Aadhaar number to share their demographic information and photograph with a UIDAI partner organization in an online, secure, auditable manner with the residents consent. The consent by the resident can be given via a Biometric authentication or an One Time Password (OTP) authentication.

What information is shared in the e-KYC service?

The Aadhaar holders demographic information i.e Name, Address, Date of Birth, Gender, Phone & Email (where available) & Photograph which is currently available with the resident is shared via the e-KYC service.

10. Who can use the e-KYC service?

The e-KYC service is envisaged as a public benefit service. Any organization, authorized and approved by UIDAI to use this service can deploy the e-KYC service to serve its business interest. UIDAI envisages, initially organisations such as Banks, Telecom, Financial Services etc who have a regulatory compliance to perform a KYC function will be the front runners in leveraging this service.

What is the process to start using the e-KYC service?

Organizations interested in using the e-KYC service, will need to get approved and authorized by UIDAI to use this service. The details of the process of making an application, supporting documents required, technical integration guidelines etc can be found at the following link:

- http://uidai.gov.in/authentication-2/more.html

What are the key features of the e-KYC service?

Some of the key features of the e-KYC service are:

- Paperless: The service is fully electronic, enabling elimination of KYC document management
- Consent based: Data is shared by the resident consent through Aadhaar authentication, thus protecting resident privacy.

- Secure and compliant with the IT Act: Data transfer are secured through the use of encryption and digital signature as per the Information Technology Act, 2000 making e-KYC document legally equivalent to paper documents.
- Non-repudiable: The use of resident authentication for authorization, the affixing of a digital signature by the service provider originating the e-KYC request, and the affixing of a digital signature by UIDAI when providing the e-KYC data makes the entire transaction non-repudiable by all parties involved.
- Instantaneous: The service is fully automated, and KYC data is furnished in real-time, without any manual intervention
- Regulator friendly: The service providers can provide a portal to the Ministry/Regulator for auditing all e-KYC requests.

What is the regulatory stance on the e-KYC service?

RBI, IRDA, PFRDA & SEBI have accepted UIDAI's e-KYC service as a valid KYC.

Training and Certification

Is training mandatory?

Training is not mandatory, however it is recommended that the people desirous of working with the Enrolment Agencies (EA) as operator , supervisor and tech support undergo the training programme (as mentioned in the Training Design structure) .

What are the plans for developing the training ecosystem in UIDAI?

• UIDAI has empanelled 15 training agencies. These training agencies are being invited for Masters Trainers workshop to be trained by UIDAI.

• The faculty members of empanelled Training Agencies- are being trained in Master Trainers(MT) Programme. UIDAI is organizing Master trainer programmes (MT) for the purpose of developing Master trainers, who in turn can replicate training. Nominations for the MT programmes are being organized from the empanelled training institutes before each programme.The list of faculty members trained in MT programmes is available on the website

• The Enrolment agencies (EAs) may get their staff trained through the empanelled training agencies

What is the Training Design Structure?

The training design structure is an indicative training outline for different role holders of the Enrollment Agencies (EA) and the other stakeholders. The duration specified are indicative in nature and are based on Training Needs Analysis (TNA) done by the agency appointed by UIDAI. The EAs can do their own assessment of the duration of training. The empanelled training agencies who have not nominated their trainers already (or got the master trainers trained) can send their nominations to following :

Ashish Kumar : ashishcoomer@gmail.com
Maneesh Mishra: maneesh.uidai@gmail.com

Who will train the EA operators, Supervisor and the tech staff?

The EAs can get their staff trained through empanelled training agencies, or through their own trainers. The staffs can also self train with the help of training material available on the website.

How will the fee for training decided ?

The fee can be decided between the EA and the TA. UIDAI does not prescribe the fee as the training needs can vary depending on the needs of the EA or the target group.

What is the duration of training?

Duration of training will depend on requirement of Registrar/ EAs. EA/TA may customise the material as per local needs and create additional content to make it Registrar specific, if required

Where can one access training content ?

It can be accessed on the website , www.uidai.gov.in under the training section. The training content is available in PDF and Computer based training (CBT) formats.

What is the Certification process for EA staff?

The candidates from different EAs will register for the test. The registration can be done on the portal http://uidai.sifyitest.com. The detailed information regarding the test and registration is available on the website.

Who will conduct the test?

Sify is the agency chosen for testing.

How will this test be conducted?

It will an Internet based testing in proctored environment at the specified test centres.

Where are the test centre located?

The information regarding the test centres is available on the portal http://uidai.sifyitest.com.

What will be periodicity of the test?

For each location the test will be conducted at-least once in two weeks.

What are the fees for taking the Certification test?

Rs. 365 per candidate per test. For retests the candidate pays 200 per retest.

How many times can I take the test?

The candidate can take test upto 3 times in 6 months.

In case I have to take a retest , would I have to pay the fee again?

Yes. Every time the test is taken the fee of Rs 365 would be applicable.

Will I have to take the retest in all the modules even If I pass a few modules in first attempt?

No, while taking the retest the candidate can appear for the module he/she could not pass in the earlier attempt.

What is the structure of the certification test?

90 minutes -, QB for 60 minutes - , and simulation test for 30 minutes. The detailed module wise test structure in available on www.uidai.gov.in under the training section.

Where do I get the list of empanelled training agencies from?

The list and contact info is available on the website under the training section.

Will there be a need of recertification?

No! UIDAI has mandated onetime certification for one role, e.g. Enrolment Operator or Supervisor

How can I Register for the test?

The registration info will be available the portal http://uidai.sifyitest.com.

Who will issue the certificate? UIDAI or Sify ?

The Certificate will be given by Sify.

Where can one access training content?

It can be accessed on the website, www.uidai.gov.in under the training section. The training content is available in PDF and Computer based training (CBT) formats.

Is testing mandatory for working as Enrolment Agency operator or supervisor under UIDAI

Yes. Testing has been made mandatory from 1st January 2011 without any exception. Data packets received from uncertified operators/ supervisors will not be processed.

Where is the question bank for the practice available?

The question bank to help the candidates practice for the test is available on the website www.uidai.gov.in under training section.

How can I familiarize myself with flow of the test flow?

The test familiarization module is available on the website http://uidai.sifytest.com

Can the EA make bulk payment of the candidates' test/retest fee?

Yes. The details for the bulk payment is available on the website http://uidai.sifytest.com

Inclusion

How will the UIDAI ensure that the poor and marginalized are covered and that there is no identity divide created as a result of this process?

Inability to prove identity is one of the biggest barriers preventing the poor from accessing benefits and subsidies. The UIDAI is committed to an inclusive enrolments where children,

differently abled persons, the poor and marginalised can also secure a unique ID. The extensive network of Registrars that have large network among the poor and rural communities such as (National Rural Employment Guarantee) NREGA Scheme ,RSBY etc will help bring large number of poor and underprivileged into UID system.

In addition, the UIDAI is also working with outreach groups to access hard to reach communities like tribal, the differently-abled, urban poor, workers in the unorganised sector.

UIDAI has also created a system of 'Introducer' to enable enrolment of residents into Aadhaar, who are not be part of any government database or who don't have valid document to prove their identity. The Registrars identify people from various walks of life such as elected members, members of local administration bodies, postmen, influencers such as teachers & doctors, Anganwadi / ASHA workers, representative of local NGO's etc. and register them in CIDR as "Introducer".

How will the biometric of the Differently-abled and people with no finger prints or rugged hands e.g. beedi workers or people with no fingers be captured?

There is a well defined process for handling exceptions in aadhaar enrolments. The biometric standards prescribed by the UIDAI takes care of that the people without hands/ fingers/ eyes etc so that no one can be deprived of the Aadhaar.

How will children be captured in the database?

For Children below 5 years of age, Aadhaar will be issue based on their parents/ guardian's Aadhaar. These children will need to re-enrol and have biometrics captured at age 5 and 15 -- the UIDAI will send a reminder letter for the same. For children above 5 years biometrics will be captured during enrolment. They will need to re-enrol at the age of 15 years – the UIDAI will send a reminder letter.

Use of the information in the UIDAI database

How will the information in the database be used?

The information in the UID database will be used only for the purpose of authentication.

What is authentication?

Authentication is the process through which the aadhaar number of a resident , along with other attributes (including biometrics) are submitted to the Central Identities Data Repository for its verification and such Repository verifies the correctness thereof on the basis of information or data or documents available with it
The response from the CIDR to a authentication query will only be a positive or a negative response, the UIDAI shall not give out the demographic or biometric information of a resident in response to an authentication query.

Who owns the data collected by the UIDAI?

The data pertaining to residents is held by UIDAI as a trustee /custodian, and is not shared with any agency without the consent of the resident, either in writing or when electronically authenticated. The Aadhaar is activated only at the request of the Aadhaar holder. He/ She may choose to let it be dormant by not using it at all. As a trusted custodian, the residents' data has always been handled in a responsible manner with state-of-the-art security systems in place in the UIDAI.

Can one de-activate one's Aadhaar?

UIDAI's update policy version 2.3 (available on the official website uidai.gov.in) has provisions for deactivation of Aadhaar, which are given below:

a. If within 2 years of attaining age 5, the child's biometrics are not updated in Aadhaar database, his/her Aadhaar number will be deactivated (no authentication permissible). It will be reactivated once biometrics are updated in database.
b. If within 2 years of attaining age 15, the child's biometrics are not updated in Aadhaar database, his/her Aadhaar number will be deactivated (no authentication permissible). It will be reactivated once biometrics are updated in database.
c. If Resident has not biometrically authenticated in 5 years, his/her One Time Password (OTP) based authentication services will be deactivated. They will be re-activated once the resident biometrically authenticates.

Protection of the individual in the UIDAI system

How does the UIDAI protect the individual and their information?

Protection of the individual, and the safeguarding their information is inherent in the design of the UID project. From having a random number which does not reveal anything about the individual to other features listed below, the UID project keeps the interest of the resident at the core of its purpose and objectives.

• **Collecting limited information**

Data collected by the UIDAI is purely to issue Aadhaar numbers, and confirm the identity of Aadhaar number holders. The UIDAI is collecting basic data fields in order to be able to establish identity– this includes Name, Date of Birth, Gender, Address, Parent/ Guardian's name essential for children but not for others, mobile number and email id is optional as well . The UIDAI is collecting biometric information to establish uniqueness – therefore collecting photo, 10 finger prints and iris.

• **No profiling and tracking information collected** The UIDAI policy bars it from collecting sensitive personal information such as religion, caste, community, class, ethnicity, income and health. The profiling of individuals is therefore not possible through the UID system, since the data collected is limited to that required for identification and identity confirmation. The UIDAI had in fact, dropped the 'place of birth' data field – part of the initial list of information it planned to collect – based on feedback from CSOs that it could lead to profiling.

The UIDAI also does not collect any transaction records of the individual. The records of an individual confirming their identity through Aadhaar will only reflect that such a confirmation happened. This limited information will be retained for a short period time in the interest of the resident, to resolve any disputes.

• **Release of information – yes or no response** The UIDAI is barred from revealing personal information in the Aadhaar database – the only response permitted are a 'yes' or 'no' to requests to verify an identity . The only exceptions are the order of a court, or the order of a joint secretary, in case of national security . This is a reasonable exception and is clear and precise. This approach is also in line with security norms followed in US and Europe on access to data in case of a security threat.

• **Data protection and privacy**

The UIDAI has the obligation to ensure the security and confidentiality of the data collected . The data will be collected on software provided by the UIDAI and encrypted to prevent leaks in transit. Trained and certified enrollers will collect the information, who will not have access to the data being collected.

The UIDAI has a comprehensive security policy to ensure the safety and integrity of its data. It will publish more details on this, including the Information Security Plan and Policies for the CIDR and mechanisms for auditing the compliance of the UIDAI and its contracting agencies. In addition, there will be strict security and storage protocols in place. Penalties for

any security violation will be severe, and include penalties for disclosing identity information . There will also be penal consequences for unauthorised access to CIDR – including hacking , and penalties for tampering with data in the CIDR .

• **Convergence and linking of UIDAI information to other databases**

The UID database is not linked to any other databases, or to information held in other databases. Its only purpose will be to verify a person's identity at the point of receiving a service, and that too with the consent of the aadhaar number holder. The UID database will be guarded both physically and electronically by a few select individuals with high clearance. It will not be available even for many members of the UID staff and will be secured with the best encryption, and in a highly secure data vault. All access details will be properly logged.

Who will have access to the UID database? How will the security of the database be ensured?

• Residents who have aadhaar numbers will be entitled to access their own information stored in the UID database.
• CIDR operations will be follow strict access protocols to limit access to the database.
• The database itself will be secured against hacking and other forms of cyberattacks

How will the grievances of the resident be addressed?

The UIDAI will set up a Contact Centre to manage all queries and grievances and serve as a single point of contact for the organization. The details of the Contact Centre will be published on the website as and when enrolment begins.
• The users of this system are expected to be residents, registrars and enrolment agencies.
• Any resident seeking enrolment is given a printed acknowledgement form with an Enrolment Number, that enables the resident to make queries about her/his enrolment status through any communication channel of the contact centre.
• Each enrolment agency will be given a unique code that will also enable faster and pointed access to the Contact Centre that includes a technical helpdesk.

Can a resident opt out of Aadhaar?

The resident has the option in the first instance not to enroll for Aadhaar at all. Aadhaar is a service delivery tool, and not designed for any other purpose. Aadhaar being unique to every resident , is non-transferable. If the resident does not wish to use the Aadhaar, it will remain dormant, as the use is based on the physical presence and biometric authentication of the person. However, currently, there is no provision to opt out of the Aadhaar database, but it must be again said here that except for the resident, his Aadhaar cannot be used by any other person.

Can the resident's data be purged from Aadhaar database?

As is the case with the other services availed from the government, there is no provision for purging the data of the resident from the database once he has obtained his Aadhaar. The data is also required as it is used for de-duplication of every new entrant in the database against all the existing records to establish the uniqueness of the resident. Only after this process is completed that the Aadhaar is assigned.

Use of Aadhaar

What use can aadhaar be put to? What are the Aadhaar enabled applications? How a resident gets benefited through Aadhaar enabled applications?

Response:
Aadhaar means foundation , therefore it is the base on which any delivery system can be built. Aadhaar can be used in any system which needs to establish the identity of a resident and/or provide secure access for the resident to services/benefits offered by the system. Aadhaar can be used in the delivery of the following programs:

- Food & Nutrition – Public Distribution System, Food Security, Mid Day Meals, Integrated Child Development Scheme.
- Employment – Mahatma Gandhi National Rural Employment Guarantee Scheme, Swarnajayanti Gram Swarozgar Yojana, Indira Awaaz Yojana, Prime Minister's Employment Guarantee Program
- Education – Sarva Shikhsha Abhiyaan, Right to Education
- Inclusion & Social Security – Janani Suraksha Yojana, Development of Primitive Tribe Groups, Indira Gandhi National Old Age Pension Scheme
- Healthcare – Rashtriya Swasthya Bima Yojana, Janashri Bima Yojana, Aam Aadmi Bima Yojana
- Other miscellaneous purposes including Property Transactions, VoterID, PAN Card etc.

1. How is Aadhaar different from any other identity issued by the government?

Aadhaar is essentially a paperless online anytime-anywhere identity assigned to a resident to cover his/her entire lifetime. The verification of his identity is done online with the help of authentication devices which connect to UIDAI's Central Identity Repository and return only a 'yes' or 'no' response to the basic query-"Is the person who he/she claims to be?" based on the data available with UIDAI.

The Aadhaar authentication service is fully functional and in use in several service delivery schemes across the country.

The Aadhaar Card or the e-Aadhaar (electronic copy of Aadhaar) are essentially given to residents to know their own Aadhaar, but are only the first step towards the actual use of the online id as explained in the preceding para.

National Identification Authority of India

What is the National Identification Authority of India?

The Unique Identification Authority of India was set up as an attached office of the Planning Commission. It is now proposed to be set up as a statutory authority by the name of National Identification Authority of India upon passage of the National Identification Authority of India,Bill 2010.

What are the key features of the National Identification authority of India Bill, 2010?

• The National Identification Authority of India (Authority) is to be set up with the purpose of issuing identification numbers (aadhaar numbers) to residents and to provide the means to authenticate aadhaar numbers to enable delivery of services and benefits to such individuals.
• The Authority shall consist of a chairperson and two part time members.
• The Authority shall have the power to develop policies, procedures and systems for issuing aadhaar numbers and authentication thereof.
• The Authority shall engage one or more entities to establish and maintain the central identities data repository, which will be the database of aadhaar numbers and corresponding demographic and biometric information.
• The Authority may appoint registrars, enrolling agencies for enrolling residents for aadhaar

numbers.
• Any resident shall be entitled to apply for an aadhaar number by providing their demographic information and biometric information.
• The Authority cannot collect information such as name, age, address of a person and cannot collect information on religion, caste, class, and tribe, Income, health of a person.
• Aadhaar number shall be a random number and once issued cannot be assigned to any other person.
• The Authority shall respond to an Authentication query with a positive or negative response.
• The Central government is to set up a Identity review committee which shall consist of three members, the function of the committee is to prepare a report (to be tabled in parliament) on the extent and pattern of usage of aadhaar number across the country and make recommendations in this regard.
• The Authority is required to ensure the security and confidentiality of the identity information of an individual.
• The Authority will be required to ensure that the information in its possession and control is protected against loss or unauthorised access.
• Aadhaar holders shall have the right to ask for their information stored in the central identities data repository and if necessary make changes and corrections from time to time.
• The information contained in the central identities data repository (including authentication records) cannot be shared with any person except if there is a court order or in case of national security upon direction of joint secretary after consent of concerned minister in charge of the department.
• Penalties are to be imposed for impersonation, for unauthorised access to the central identities data repository and for hacking or attempting to hack into the central identities data repository.

Aadhaar time frame

What is the anticipated time for receipt of Aadhaar number after the enrolment?

The waiting time for Aadhaar may vary from 60-90 days after receipt of resident data packets in CIDR. However, it could take even longer in case enrolment is done through NPR exercise.

After enrolment, quality checks are done by the enrolment centre supervisors, followed by correction process (where required) and data packet consolidation. Subsequently, the Enrolment Agency sends the data to UIDAI data centre. The data undergoes various stages of screening and validations in CIDR. This ensures that the source of data is authenticated besides ensuring that no duplicate exists. Sample Quality checks are done on demographic and biometric data collected from residents. Apart from that the Operator/Supervisor/Introducer/Enrolment Agency and Registrar information in each packet

is also validated. Only after passing the data quality checks and other validations, the packet goes for de-duplication and Aadhaar gets generated.

In case of any errors, the packet goes on hold. For example if the particulars of the Operator who enrolled the resident are found to be inconsistent with database or there is a mismatch observed in photo and age/gender (ex. a child's photo with age mentioned as 50 yrs), then the packet is held for further enquiry. Corrective actions are taken on such packets, wherever possible, else a rejection letter guiding resident to re-enroll is dispatched to the resident. India Post is entrusted with the responsibility of printing and delivery of Aadhaar letters. Depending on backlog for generation, location of delivery etc. India Post may ordinarily take 3-5 weeks to print and deliver Aadhaar letters to the residents.

In the case of Aadhaar enrolments through NPR exercise, the method of verification is the RGI approved LRUR(Local Register of Usual Residents) verification process. The Aadhaar number will be issued only after completion of the LRUR process which could take much longer than the time prescribed above. Residents can verify the name of their Registrar at the enrolment centres or on the acknowledgement provided to them at the time of enrolment. In case it is Registrar General of India(RGI), please contact office of RGI for further details.

Aadhaar authentication For Residents

What is Aadhaar authentication?

Aadhaar authentication is the process wherein Aadhaar number, along with other attributes (demographic and/or biometrics and/or OTP) is submitted to UIDAI's Central Identities Data Repository (CIDR) for verification; the CIDR verifies whether the data submitted matches the data available in CIDR and responds with a "yes/no". No personal identity information is returned as part of the response.

When do I need to authenticate?

Various service providers, such as PDS, NREGA, banks, are expected to link Aadhaar authentication to their services. Residents would need to authenticate either at the time of subscribing to the service or at the time of availing service delivery, as required by the service providers. This would benefit the residents as no one else can avail the benefits meant for a particular resident.

What are the benefits of Aadhaar authentication?

The purpose of Authentication is to enable residents to prove their identity and for service providers to confirm that the residents are 'who they claim they are' in order to provide services and benefits.

From where can I authenticate?

Authentication requests will be initiated at the point of service delivery by agencies using Aadhaar authentication. Examples include FPS shops, NREGA centres, bank terminals, education institutions and so on. Some of these touch points may be "assisted" (an operator handles the device) or as a "self-service" (kiosks, mobile phones, Internet terminals, etc.).

How can I authenticate?

To authenticate, residents should provide their Aadhaar number & other authentication attributes as requested by the service provider (fingerprint, OTP, name, address, age/DOB etc – either singularly or in combination). The request can be initiated from either a hand held device, laptop/desktop or mobile phone & sent to UIDAI's CIDR for authentication.

What does online authentication mean?

Online authentication implies that data submitted is matched against data available in a central database (vs. offline authentication, where data submitted is matched against data stored locally such as smart card or data on the device itself).

How is Aadhaar authentication different from smart card authentication?

In Aadhaar authentication, Aadhaar number of a resident & the data to be authenticated is sent online to UIDAI's CIDR for matching against data present in CIDR.
In smart card authentication, the data/biometric is checked against data stored in the smart card. Aadhaar online authentication will have certain distinct advantages over offline authentication in terms of being more cost effective, more secure and allowing portability.

Through Aadhaar authentication, can someone find out my personal information?

No. CIDR only returns "Yes/No" after matching the data submitted along with the Aadhaar number.

What all data can be authenticated / verified with UIDAI?

UIDAI provides demographic data verification & biometric authentication. Demographic data that can be verified includes data captured as part of enrolment – name, address, gender, age/DOB, mobile number, email address. Biometric authentication can be done through fingerprints or iris. In addition, UIDAI also provides OTP based authentication.

Is there a mechanism to notify the residents when an authentication occurs against their Aadhaar number?

UIDAI has an sms and email based notification mechanism. Through this mechanism, every time CIDR receives an authentication request against an Aadhaar number, a notification will be sent to the registered mobile / email address.
UIDAI will also provide a facility wherein residents can request the history of authentication requests for a specified period of time

Can I choose whether or not to receive notification when someone authenticates me?

For biometric & OTP authentication, notification will necessarily be sent to the registered mobile and email address.For demographic data verification, residents can choose whether or not to receive notifications.

I received an authentication notification even though I did not authenticate myself. Whom do I approach?

The authentication notification will contain the name of the service delivery agency through which authentication request was received. Residents are advised to approach the respective service delivery agency.

What if my authentication request gets rejected even though I provide my biometrics/demographic details with my Aadhaar number?

If biometric authentication fails, residents can retry multiple times with different fingers, appropriate pressure and cleaning the sensor / their fingers.
If biometric authentication fails repeatedly over a period of time, resident may need to approach an Aadhaar updation centre and get biometrics updated with CIDR. Resident may also go for Best Finger Detection (BFD) which will guide on the next steps.
If demographic authentication fails, request should be resent after entering correct data – as provided to UIDAI at the time of enrolment & as printed in resident's Aadhaar letter.

What is Best Finger Detection (BFD)?

Success of biometric authentication is dependent on the quality of biometric captured in the authentication request and at the time of enrolment. The quality varies across different fingers of a resident, amount of pressure applied etc. To educate residents on their suitable fingers for biometric authentication, UIDAI has developed a protocol called BFD.
BFD application requires a resident to provide biometric authentication through each of the ten fingers one-by-one. All ten fingerprints along with the Aadhaar number are sent to CIDR, which in turn returns a response indicating which fingers are best suited for Aadhaar biometric authentication.
Based on the fingerprint quality analysis, the resident may also be advised to update their biometrics with CIDR. For further details, residents can contact UIDAI's contact centre.

Do I need to undergo BFD before every biometric authentication?

No. BFD or resident on-boarding is expected to be a one-time exercise, preferably before a resident does first biometric authentication.

Where can I get BFD done?

Every AUA is expected to deploy BFD application on their devices, which would be an integral part of the authentication device / application.

What if I authenticate with a finger other than the "best" finger identified by the BFD tool?

BFD helps improve chances of successful authentication with minimal number of attempts. If a resident authenticates if a finger other than the "best" finger, the authentication packet will still be processed. If the authentication transaction succeeds, the required service would be delivered. If the authentication fails, resident may try with another finger.

Will I be denied my entitlements (ration, NREGA job etc.) if my authentication request is rejected?

UIDAI and the service providers availing Aadhaar authentication recognize the fact that Aadhaar authentication is subject to certain technological and biometric limitations such as false accepts, false rejects, network availability etc. To counter the same, the service providers will have alternate processes to identify/ authenticate their beneficiaries/ customers. Residents should not be denied entitlements due to technological or biometric limitations.

How will I authenticate if my fingerprints are worn out / I have no fingers?

Service providers are advised to deploy alternate authentication mechanisms including Aadhaar OTP to handle such issues.

How do I request for OTP?

OTP can be requested through service providers' application requiring OTP authentication, mobile number registered with CIDR, Aadhaar portal or Aadhaar contact centre.
OTP will always be delivered to registered mobile and/or email.

I do not have mobile / email. How will OTP be delivered to me?

In the context of Aadhaar, usage of OTP adds the factor of "possession of mobile/email address" as a way to strengthen the authentication. Hence OTP will not be available as an option for residents who have not registered their mobile number or email with Aadhaar system.

Aadhaar authentication For AUAs & ASAs

What is Aadhaar authentication?

Aadhaar authentication is the process wherein Aadhaar number, along with other attributes (demographic and/or biometrics and/or OTP) is submitted to UIDAI's Central Identities Data Repository (CIDR) for verification; the CIDR verifies whether the data submitted matches the data available in CIDR and responds with a "yes/no". No personal identity information is returned as part of the response.

What are the expected benefits of Aadhaar authentication? How to use Aadhaar authentication as part of service delivery?

Some of the expected benefits of Aadhaar authentication are:
• Establishing identity for purposes such as adding new beneficiaries, confirming genuine beneficiary before service delivery, attendance management, financial transactions etc.
• Enabling demand-driven, portable service delivery by providing anywhere anytime real-time authentication
• Access to relevant MIS and empowerment of beneficiary
• Improving efficiency & transparency in service delivery by enabling tracking of end-to-end service delivery process, improving accountability and vigilance etc.
• Access control to restricted areas such as airports, hotels, high security buildings etc.

Aadhaar authentication may be used at various points in service delivery when there is a need to authenticate / identify / audit / hold accountable beneficiaries, officials or other members of service delivery / monitoring / audit chain. Illustrative details on how Aadhaar authentication may be integrated in various service delivery programs such as PDS, NREGA, JSY, SSA etc are available in various working papers and presentations developed by UIDAI.

What all data can be authenticated / verified with UIDAI?

Aadhaar authentication supports demographic data verification & biometric authentication.
Demographic data that can be verified includes data captured as part of enrolment – name, address, gender, age/DOB, mobile number, email address.
Biometric authentication can be done through fingerprints or iris.
In addition, UIDAI also supports OTP based authentication.

How can Aadhaar authentication be used for cleaning up database(s)?

Aadhaar fundamentally provide two values – uniqueness and online authentication.
Uniqueness attribute can be used to eliminate ghosts & duplicates, if any, from databases.
Online authentication for demographic data such as name, address, age/DoB, mobile number and email address can be used for keeping database up to date and clean.

How is Aadhaar authentication different from smart card authentication?

In Aadhaar authentication, Aadhaar number of a resident & the data/biometric to be authenticated is sent online to UIDAI's CIDR for matching against data present in CIDR.
In smart card authentication, the data/biometric is checked against data stored in the smart card.
Aadhaar online authentication will have certain distinct advantages over offline authentication in terms of being more cost effective, more secure and allowing portability.

How can an AUA use Aadhaar authentication services to seed Aadhaar in their database?

An AUA can request Aadhaar holders to provide their Aadhaar numbers, for seeding in the database, before service delivery. An AUA can further verify the correctness of the Aadhaar numbers, so provided, through demographic and/or biometric authentication of the Aadhaar holders.

Is resident involvement mandatory for every Aadhaar authentication?

Resident involvement is not necessary for demographic authentication, wherein an AUA can verify demographic attributes such as name, age/DOB, address, gender, mobile number, email address available in AUAs' database. However, for biometric and OTP authentication, resident involvement is necessary for every authentication transaction.

Is resident involvement mandatory for every Aadhaar authentication?

Resident involvement is not necessary for demographic authentication, wherein an AUA can verify demographic attributes such as name, age/DOB, address, gender, mobile number, email address available in AUAs' database. However, for biometric and OTP authentication, resident involvement is necessary for every authentication transaction.

Do the names/addresses of beneficiaries/ customers in AUA database need to be spelled same as that in CIDR for verification?

Not necessary. Aadhaar authentication supports exact match and partial match. Partial match implies that based on a threshold that an AUA sets, name "Ram Kumar" can be authenticated as "R Kumar" OR "Ram K". For partial match, at least spelling of one word should match exactly. Similarly, for address, the verification can be either entire address verification or partial at state, district, pin code, village / town/city, locality, house number level.

What all authentication factors is UIDAI supporting?

Besides demographic data verification, UIDAI offers following factors of authentication for cases where it is required to prove "who you say you are":

- Who you are (inherence factor) – biometrics
- What you have (possession of mobile) – OTP

Can an AUA use one authentication factor from UIDAI & another one from itself?

Yes. UIDAI advocates federated authentication system wherein, the AUAs are encouraged to use Aadhaar Authentication in conjunction with the AUA's existing authentication system. Aadhaar authentication will supplement & work in conjunction with existing authentication systems to strengthen the overall authentication rather than replace existing authentication systems.

How many fingers should be used for authentication?

One or more fingers can be used for an authentication transaction.

Can Aadhaar authentication be combined with ATM/card based authentication? If yes, how?

Yes. An AUA is free to combine multiple authentication factors for strengthening the authentication services / fulfil other service/business/regulatory needs.

How many fingers should be used for authentication?

One or more fingers can be used for an authentication transaction

What does an AUA need to do to use Aadhaar authentication?

Key steps to be followed include:
- Identify business / service delivery needs and select appropriate authentication types
- Fill online application form
- Engage with ASA(s)
- Send signed contract and supporting documents to UIDAI
- Ensure process and technology compliance
- Plan device deployment
- Obtain approvals from UIDAI
- Carry out end-to-end testing
- Go-live

Is it necessary for an agency seeking to utilize Aadhaar authentication for its service delivery to have direct agreement with UIDAI?

Aadhaar authentication ecosystem has provision wherein any agency seeking to use Aadhaar authentication of its customers/associates etc for service delivery can engage with an existing AUA. Such agencies which enter into agreements with AUA are defined as Sub-AUA. Any agency wanting to become an AUA needs to have an agreement with UIDAI directly.

What is the extent of process & technology re-engineering required for using Aadhaar authentication?

To reap maximum benefits from Aadhaar authentication, AUAs may re-engineer some of their processes and technology. AUAs could use Aadhaar authentication to not only verify their beneficiaries / customers but also improve efficiencies in their entire supply chain. Adoption of Aadhaar authentication may also provide an opportunity to various service delivery agencies to review and improve their service delivery model.
At the minimum, AUAs would need to identify points in their service delivery where Aadhaar authentication may be integrated and then ensure the technology and processes are integrated for doing the same.
The details of technology re-engineering required are available on technical FAQs, API & other technical documents present on UIDAI's website http://uidai.gov.in/.

Can someone help me with the process & technology re-engineering?

UIDAI has empanelled certain consulting and software development companies who may be roped in for the required support.
AUAs are also free to either use in-house skill set or carry out their own tendering and procurement process for hiring services of entities that may help with technology re-engineering.

Will UIDAI provide the client application required for doing authentication?

UIDAI provides API documents and reference implementations. AUAs need to develop client application based on their requirements related to service delivery, authentication interface, probable devices etc.

Are there any specific application components that need to be included in authentication client application?

Besides the authentication application, which is based on AUA's business needs and UIDAI's authentication API, the authentication devices should have following applications:
- Best Finger Detection (BFD) application
- OTP application
- Exception handling provisions

What is resident on-boarding process?

One of the known limitations of biometric technology is false rejections. To minimize the same and provide residents an opportunity to understand their biometrics better before doing authentication, UIDAI proposes a resident on-boarding process. This will also help manage resident expectations and provide guidance to AUAs for exception handling requirements, if any.
To minimize the same and provide residents an opportunity to understand their biometrics better before doing authentication, UIDAI proposes a resident on-boarding process to be implemented by AUAs. As part of this process, when resident approaches an AUA for biometric authentication for the first time, BFD is carried out and resident is advised of this best finger(s) for authenticating. If required, a resident may also be advised to approach an Aadhaar updation centre to update his/her biometrics.

When should BFD be done? How will an operator know when to initiate BFD application?

BFD or resident on-boarding is expected to be a one-time exercise, preferably before a resident does first biometric authentication. BFD application should be integrated with the overall service delivery application and should be initiated based on a certain API error code returned by CIDR.

Does an AUA need to set up dedicated centres for BFD / Resident on-boarding?

No, BFD / resident on-boarding may be carried out through the standard service delivery authentication devices that an AUA deploys. BFD is done through a single fingerprint scanner. Other details of BFD are available in the BFD API document.

What is OTP application?

If an AUA opts for Aadhaar-based OTP authentication, the AUA should build a module for initiating OTP request and integrate the same with its service delivery application. The API for developing OTP request application is available on UIDAI's website.

What are exception handling provisions and why are they required?

The device application should have provisions to service genuine residents who may be falsely rejected during biometric authentication. Also, there should be measures to continue

service delivery in case of other technological limitations such as network non-availability, device breakdown etc. There should be no denial of service to residents due to technology limitations. The exception handling mechanisms should be backed up by features to log and track requests handled through exception handling mechanism to prevent any fraud attempts.

What kind of devices need to be used?

An AUA can choose a suitable device form & factor depending on its deployment environment and other service delivery / business need. For biometric authentication, AUA would need to adhere to sensor and extractor SDK specifications provided by UIDAI. These sensors and extractors can be integrated with device form and factor suitable to AUA.

Would UIDAI be certifying devices? If yes, how?

Certification is required only for the sensor and extractor combinations required for biometric authentication. Overall devices will not be certified. The certification will be done by a STQC. The certification process would be similar to that of enrolment biometric devices. The details are on http://www.stqc.gov.in/.

Does each device need to be registered with UIDAI / CIDR?

As part of public devices and currently published authentication specification, registering each device is not required. In the future, as specifications change, this may be required. UIDAI will publish updated specifications and processes.

Is there any certification mechanism for the authentication device operators?

Not as of now. Training & certification of operators/devices depends on AUAs business model and rules. Based on those, AUAs may choose to train and certify operators and other partners in their network.
In case an AUA opts for biometric authentication, some key areas that should be part of operators' training include:

- Usage of biometric devices and Do's / Don'ts for capturing good quality biometrics
- Usage of BFD, process for on-boarding residents and guiding residents for next steps
- Exception handling processes and ensuring no denial of service to residents due to technology limitations
- Fraud monitoring & fraud reporting mechanisms
- Basic troubleshooting steps and contact details of AUA's device/application support team

Do the operators need to get registered with UIDAI / CIDR?

Not as of now. AUAs are expected to manage all partners and users within their network for conducting transactions. UIDAI offers just authentication and how it is used within the business transaction is based on the AUA application and rules.

How can devices be connected to servers for authentication? Any leased line required?

Remote devices should be able to send authentication request to AUA servers over various types of networks – mobile network, PSTN, broadband. UIDAI mandates a leased line only between ASA and CIDR.

What is the expected turnaround time for authentication response?

Under normal circumstances (depending on the choice of network by the AUA), the expected turnaround time is about 1 second to 10 seconds.

How to carry out authentication if network connection is down?

For cases where connectivity is intermittent or connectivity is a little distance away, UIDAI has a solution called "buffered" authentication wherein authentication request may be "buffered" (or queued) on the device until a pre-specified period of time and then sent to CIDR for authentication when connectivity is restored / available.

What is buffered authentication?

Buffered authentication is a type of online authentication where requests are queued up at the device for a short time (currently up to 24 hours) and sent to CIDR when connectivity is restored. Buffered authentication may be used in situations where connectivity is intermittent or connectivity is a little distance away.

Who are the ASAs that an AUA can approach for carrying out Aadhaar authentication?

ASAs are entities with secured lease line connectivity with UIDAI CIDR. There are distinct advantages of having ASA such as better manageability, more security, and provision for AUA to focus on service delivery rather than establishing lease line connectivity etc.The list of approved ASAs will be available online. An AUA can choose to engage with any of the approved ASAs. An AUA may become its own ASA as well by establishing leased line and completing rest of the process-technology integration.

Can ASAs charge money for enabling Aadhaar authentication?

Yes, ASAs can charge for the services they offer to AUAs. By enabling several ASAs and also allowing AUAs to connect directly, UIDAI will ensure choice and healthy competition.

How can an entity become an ASA?

The qualification criteria for becoming an ASA are published on UIDAI's website. Any entity fulfilling the criteria and interested in becoming an ASA needs to do the following:

- Fill online application form
- Send signed contract and supporting documents to UIDAI
- Establish leased line connectivity with CIDR
- Ensure process and technology compliance
- Obtain approvals from UIDAI
- Carry out end-to-end testing
- Engage with AUAs

Who all can connect to "Public authentication URL" offered by UIDAI?

This is provided only for testing purposes. This is not expected to be used for production. The URL is http://auth.uidai.gov.in/

What kind of contracts, obligations do AUAs/ASAs need to sign/understand?

Both AUAs and ASAs need to sign contracts with UIDAI. The contract between AUA and ASA is the discretion of signing parties. UIDAI has a set of proposed guidelines that may be included in the contract between an ASA and an AUA. However, the contract (and commercial terms, if any) between an ASA and an AUA is at the sole discretion of the signing parties and UIDAI does not have any responsibilities regarding same. Similarly, if an ASA provides any value added services to an AUA over and above Aadhaar authentication, UIDAI will not be party to any such services.

Aadhaar authentication Financial Inclusion

Will an Aadhaar Enabled Bank Account (AEBA) be opened with every issue of an Aadhaar number?

AEBA will be opened for every resident who chooses to do so at the time of enrolment.

Can the existing bank accounts also be linked to Aadhaar?

Customers can link their existing bank accounts to Aadhaar by contacting their bank. All banks are in the process of implementing Aadhaar-linkage processes.

How will an Aadhaar enabled bank account help a resident that already has a bank account?

It is envisaged that disbursement Electronic Benefit Transfer (EBT) payments and Direct Transfer of Subsidy (DTS) payments will be transferred into Aadhaar-enabled accounts. This includes social security benefits like pensions, scholarships, MGNREGS wages, LPG subsidy, Fertilizer subsidy, etc.

What is an Aadhaar Enabled Bank Account (AEBA)?

Aadhaar-enabled bank account (AEBA) is a bank account linked to Aadhaar number of the resident that allows transactions on the basis of resident's Aadhaar number.

What is the Aadhaar-Enabled Payments System (AEPS)?

The AEPS is an interoperable network of microATMs that is operated by the National Payments Corporation of India (NPCI). It will enable the following interoperable transactions:

Cash withdrawal
Cash deposit
Balance enquiry
Remittance

Further details are available at http://www.npci.org.in/AEPSOverview.aspx

What are micro-ATMs? How will they work in the Aadhaar system?

Micro-ATMs are compact payment devices that are operated by a BC or BC sub-agent appointed by Banks. The micro-ATM standards are published at http://uidai.gov.in. Micro-ATMs will enable the following interoperable transactions:

Cash withdrawal
Cash deposit
Balance enquiry
Remittance

What is the Aadhaar Payments Bridge (APB)?

APB is a backend payments processing platform that allows Government agencies to transfer funds into AEBA using only an Aadhaar number, and the amount to be transferred.

How can an agency use APB for transferring funds to be disbursed to their beneficiaries?

The key requirements for an agency to start using APB are:

a. Seed Aadhaar in their beneficiary database. This requires mapping Aadhaar number to the welfare scheme number such as MGNREGA job card number.

b. Ask their bank to work with NPCI and obtain Institutional Identification Number (IIN) and integrate APB with their system.

c. Create APB file containing Aadhaar number, bank IIN, amount and welfare scheme reference number and provide to their bank.

Does a service delivery agency need to sign any contract / engage with any specific organization(s) to post payments via APB?

The service delivery agency needs to engage with their bank to avail of APB. The bank in turn gets the agency registered with NPCI.

Does a service delivery agency necessarily need to become AUA to use APB / AEBA / AEPS?

Service delivery agency need not become AUA to use APB / AEBA / AEPS. The bank that will have AEBA and offer AEPS to its customers would need to become an AUA / sub-AUA of UIDAI.

What does a bank need to do to avail APB/AEPS?

To become a member of APB, banks need to work with NPCI. To use AEPS, banks need to become AUA / sub-AUA of UIDAI as well as work with NPCI for overall integration.

Registrar

Who is a Registrar?

"Registrar" is any entity authorized or recognized by the UID Authority for the purpose of enrolling the individuals for UID numbers. Registrars are typically departments or agencies of the State Government/Union territory, public sector undertakings and other agencies and organizations, who interact with residents in the normal course of implementation of some of their programs, activities or operations. Examples of such Registrars are Rural Development Department (for NREGS) or Civil Supplies and Consumer Affairs Department (for TPDS), insurance companies such as Life Insurance Corporation and Banks.

Registrars will collect demographic & biometric data from residents directly or through Enrolment Agencies. Registrars have the flexibility to collect additional data, which will be referred to as 'KYR+' fields for the various applications they have in mind.

The UIDAI has developed standards, procedures and processes, guidelines and technology systems to execute the entire Aadhaar enrolment process which will be adhered to by the Registrars. Registrars can also leverage the Ecosystem that has been built by the UIDAI in order to support them in this process.

How does the Registrar get started on UIDAI project?

The UIDAI has also defined a detailed Registrar Onboarding Process and Guide in order to support Registrars across the stages of becoming Aadhaar Ready. A high level summary of it is in this document:

1. Setting Up Committees and Joint Working Groups

- Set up Apex/ Empowered Committee headed by CM and an Implementation Committee headed by Chief Secretary. It is recommended that UIDAI Regional Office and State UIDICs must coordinate with the State Registrars (SRs) and Non State Registrars (NSRs) in their States to increase accountability across stakeholders and facilitate the working of NSRs in tandem with SRs.

Identify Nodal Department for Aadhaar; **Identify Departments which will act as Registrars along with a nodal Officer**. Other Departments which are not included as Registrars in the project at the time of enrolment, will have the option of 'Aadhaar enabling' their systems at a later date. The Nodal and the Registrar departments can be the same department or different departments.
Ensure MoU is signed
Identify Agency for Receiving financial assistance for enrolment: The UID Authority provides some financial support to its Registrars per successful enrolment into the UID system. To operationalise this arrangement, the Registrars will have to provide the details of the Registrar (name and account details) through which they would like to receive the amount.
Setup Joint Working Group – headed by the Head of the Nodal/Registrar Dept. The other members should be Officers, who can lead the Technology, Process, IEC, Applications teams from the Registrar's side. UIDAI will nominate appropriate representatives to assist the State Government/Registrars in carrying through the entire process. Bank representatives may be included where the Financial Inclusion (FI) solution is a part of enrolment.
Ensure smooth functioning and active participation of the working group during UIDAI – Registrar alignment.
Ensure deliverables / project plan activities as mentioned in the UIDAI Registrar Readiness Checklist (RRC) are executed. Update RRC along with UIDAI nodal officer and EA at each stage. Hand over the signed checklist to Regional Office/Nodal Officer.

2. Sensitization Workshops

A series of sensitization workshops are held to provide an overview of Aadhaar, enrolment and IEC approach, roles and responsibilities at State/District/ Village levels, enrolment strategy and plans.
This will be followed by a set of sub-group workshops and meetings with members of the process, technology, IEC and applications teams respectively to identify the key areas of integration and implement the same. Ensure that Registrar's technology, process & IEC aspects are aligned with UIDAI.
A "Go Live readiness Workshop" will be scheduled 2-3 weeks before scheduled 'go-live' date to take stock of the implementation status on items required to start enrolments.
Registrar must advise UIDAI's focal point on modalities for setting up the on-boarding workshop and should ensure that the required stakeholders and members of working group attend the workshop.
Define the role of Civil Society Organizations (CSOs) in the enrolment process and develop a panel of CSOs at the local level who can help enrol marginalized communities. Social Inclusion is a mandatory requirement for registrars. Special enrolment drives should be initiated by registrars in consultation with ROs for the underprivileged, various vulnerable groups and disabled persons.

What are the Responsibilities of the Registrar under the Aadhaar Project?

A high level summary of various roles and responsibilities of Registrar are:

1. **Enrolment Planning**

As a part of the Enrolment Planning workshop, the Registrar is advised to finalize the **targeted enrolment** nos., locations to be covered and timelines for the same. This data can in turn be used to plan the no. of Enrolment Stations needed, locations for the same, devices needed, operators to be staffed etc.
Registrars will also decide **enrolment approach** (phased, sweep etc). It is strongly recommended that the Registrar enrol all residents of the locality and not limit it to their beneficiaries/ customers. 'Sweeping' all residents will give Registrars the benefits of economies of scale and optimizing on the cost of enrolment per resident.
Finalize plan to **include marginalized/vulnerable** communities & areas for CSO involvement. Special enrolment drives should be initiated by registrars in consultation with ROs for the underprivileged, various vulnerable groups and disabled persons.
Identify area of interest for **Aadhaar-enabled applications**. Identify govt remittances which can be routed through Aadhaar-enabled Bank accounts. Registrars should link their UID enrolment activities to their core programs and citizen centric service delivery.
Registrar will work with the UIDAI to identify Banks to partner with for **Financial Inclusion** solution. Define processes as required to implement the Financial Inclusion solution.
At times, Registrar's may have to hold special camps or call residents for re-enrolment like in case where EA machines get stolen or where Resident data packets are irrecoverable due to process/technology failure. Registrar must keep the EA apprised that such situations may arise and they have to be prepared for re-enrolment of residents in such cases.
Registrar must keep the local authorities, Introducers, Verifiers and other stakeholders informed of enrolment schedule

In order to start enrolments, the Registrar has to complete the following activities, many of which can run in parallel and would have commenced post the Project Initiation Workshop:

2. **Enrolment Agency Selection and On-boarding**
Identify Enrolment Agencies (EA)
1. Registrars may engage Enrolment Agencies for the purpose of enrolling resident into Aadhaar. Registrars will share the details of hired Enrolment Agencies with UIDAI.
2. Registrars are advised to engage only Empanelled Enrolment Agencies. If non-empanelled agencies are engaged, they must be subject to the same terms and conditions as the empanelled agencies.
3. New contracts should include a clause of continued empanelment mandatory for continuation of work. Model RFP/Q templates and the list of empanelled agencies have been published on UIDAI website.
4. **No Sub Contracting** – Subcontracting has serious impacts on the quality and security of data. Agreement with enrolment agencies should have conditions to discourage sub-contracting. However field level manpower such as enrolment operators and supervisors can be hired through third parties. EAs should be asked to provide details of the companies from which they are going to hire this manpower.
Onboard EA - EA Project & Technology managers need to be identified and added in JWG. Initiation Workshop for EA needs to be held by Registrar and UIDAI to provide detailed enrolment process & implementation overview.
Identify Enrolment Agency related requirements of EA training, device/resource capacity planning.
Procure infrastructure and equipment including certified biometric devices as per standards defined by the UIDAI, through the designated enrolment agencies.
It is recommended that the Registrar must insist on Enrolment agencies using only trained operators/supervisors. All Enrolment Operators need to be tested and certified; keeping in mind the significant impact they have in collecting good quality and accurate data from residents.

3. **Enrolment Centre and Stations**
Enrolment Centers and their Location
1. Registrar will identify and co-ordinate for suitable locations where Enrolment Centers may be setup keeping in mind law and order, terrain, local weather conditions, security, power availability, approach/access to the area and lighting. Refer Resident Enrolment Process document for Centre selection guidelines.
2. **Non-state registrars** should work in coordination with ROs and state nodal departments. NSRs should also have enrolment centres only in and around their premises to ensure close supervision. Bank NSRs can also be allowed to enrol through special camps provided that they have cleared these enrolment plans with the State UIDIC &/or the State Nodal officer.
3. Registrars should plan for setting up **permanent enrolment centres**. Registrars need to maintain at least a skeletal enrolment network in their respective locations, after the 'enrolment sweeps' are completed to facilitate on-going enrolments and updation.
Decide Number of Stations for Each Centre
1. The number of stations can be decided based on the target number of days for completion of enrolment in the particular area or the district and the expected number of enrolees in the area. Model RFP published on UIDAI website provides an excel sheet for facilitating calculation of number of stations.
2. Tables, lighting, backdrops, height of table, chairs, positioning of resident and operator,

and issue of direct sunlight for photo capture, all these need to be considered for enrolment station setup.
3. Ensure Setup & registration of enrolment stations as Active production machines with UIDAI. The enrolment agencies may be asked to submit their machine deployment plans and their preparedness as per a prescribed checklist. ROs will assess the preparedness of the Registrars and EAs and may then allow the on-boarding of stations.
4. Registrar must Review the **Enrolment Centre Setup checklist with Enrolment Agency** and verify if all required activities are completed.

4. Define KYR+ fields

The AADHAAR Enrolment Client application captures the KYR (Know Your Resident) data. The registrars may require capturing some other registrar specific fields related to residents called as KYR+ data. For example, in case of PDS data, information such as APL (Above poverty line), BPL (Below poverty line), Family Details, etc. may be collected as part of KYR+ data. If any KYR+ fields are to be collected, define those fields and initiate technology integration with respect to data capture API and logistics. However, experience suggests that the number of fields proposed to be captured at the enrolment station must be kept at minimum as residents cannot be expected to bring multiple documents at the time of enrolment.

5. Pre-Enrolment Data

Registrar may want to complete the demographic data capture and verification ahead of the biometric capture. This step is called pre-enrolment. In case where Registrar has a good database, Registrars can share this with Enrolment Agencies to pre-populate the AADHAAR Enrolment Client. This data would reduce the effort and time of the enrolment operators during data capture process at the enrolment centres during resident's presence. The details of the database need to be discussed and sent to UIDAI in advance in prescribed format and aligned to UIDAI requirements. However, pre-enrolling residents is not mandatory.

6. Check Pin Code Master

Registrar must Review and get Pin code master data corrected and completed prior to start of enrolments in the region. Registrar should provide list of PIN codes to be corrected in PIN codes master to UIDAI using existing Pin Code correction process.

7. Review list of Approved documents

UIDAI has defined a list of valid documents to be used during Aadhaar enrolment process as Proof of Identity (PoI), Proof of Address (PoA), Proof of Relationship (PoR) and Date of Birth (DoB). However, UIDAI and Registrars have the authority to amend and enlarge the list of PoI and PoA documents in some exceptional circumstances. Registrars may add any other required document not in the list, in consultation with UIDAI Regional Office. The Enrolment Agencies will then download the master for documents in the client stations, pertaining to the Registrar, for use during enrolment.

8. Send local language requirements

Send local language requirements for contact centre, enrolment client (label/text, transliteration). Complete local language translation for labels, print receipts/letter in coordination UIDAI.

9. Biometric data need of registrar identified

Registrars may analyse their requirement for resident data and capability to securely manage and store data. It is not necessary for Registrar to store resident's biometric data. Registrars are, instead, encouraged to adopt online authentication offered by UIDAI – this will require no local/offline storage of biometric data in registrar applications. However, if the Registrar decides to store the biometric data, then Registrar will have to share a plan to retrieve, manage and store data with UIDAI, for UIDAI to start creating Registrar data packets.

10. Provide registrar public key for data encryption

Registrars must provide their public key to the UIDAI for the purpose of encrypting the EID-UID mapping file that UIDAI will share with Registrars after Aadhaar generation. Encrypting using Registrar's public key provides a layer of security and is prescribed by UIDAI for data transfer. Registrar must contact UIDAI for details on public/ private key requirements.

11. Decryption Utility

Registrars must develop their own decryption utility for decrypting the EID-UID mapping file. Registrar should also successfully test file decryption.

12. Develop Registrar Technical requirements

Registrar will require technical personnel/system integrators for developing their technical requirements for
Pre-enrolment data capture
KYR+ application
Document storage
Registrar packet transfer/ management & usage
Decryption utility
First mile i.e. data transfer from Enrolment Centres to UIDAI and Registrar
KYR+ data transfer, automating EID-UID mapping in KYR+ database
Receiving EID-UID mapping file from CIDR. Registrar must be ready to receive and update Registrar DBs with EID-UID mapping
Other activation and portal workflow related requirements

13. Other Technology side Requirements

There are some requirements that the Registrar will need to do for integration with UIDAI database:
Get set up as a Registrar in UIDAI database. Send requisite details in prescribed format to UIDAI.
Receive Registrar code, login and password for technology portal and SFTP application
Then Attach EAs on technology portal to establish Registrar – EA linkage.
Update and activate Introducers list on technology portal
Receive and download SFTP application
Define Location Codes – Registrar can assign location codes to each of its schedule and this code can be used by Enrolment Agency in client machines when conducting enrolments in the particular region. The assignment of location codes will help in generating enrolment reports by location code which can be helpful for payment purposes. Registrar's supervisors at Enrolment Centres will have to monitor the use of correct location codes by Enrolment Agency.
A representative of the registrar performs the system configuration and registration once the software is installed. Normally the Registrar may ask the EA to perform the installation and configuration. In such a case, the configuration and Registration may be done in presence of Registrar's representatives and/or Registrar must regularly check the registration details on the client like location code, Registrar and EA name etc.
Work flow related requirements – At times Registrar may be asked to intervene and given a role in a process workflow for example in cases where resident data packets are on hold due to specific reasons. Registrar will have to complete the given responsibility in a defined time period in such cases.

14. Registrar software readiness and their integration to Aadhaar software

Registrar must check Aadhaar Application Software is ready for deployment with pincode data corrected, registrar public key and local language support included. Test Registrar's own software and their integration with Aadhaar software.

15. Information, Education & Communication

Registrar will define an integrated IEC Plan & Material leveraging the content developed by the UIDAI. The UIDAI's IEC guidelines list in detail the different kinds of stakeholders to engage (PRI members, introducers, CSOs, etc.) and the recommended messages and media to use for each of them. The IEC plan lists the activities to be triggered 45/30/15/ 7 days before commencing enrolments.

Registrars must coordinate with UIDAI IEC team for details on their IEC responsibilities.

16. Identify and Deploy Introducers

Registrars will need to identify Introducers who can help enroll beneficiaries who lack PoA/PoI documents.
Registrar identifies introducers region wise and prepares list by District/State in which the Introducer is authorized to work. Registrars can also leverage CSOs to better reach

marginalized residents, act as Introducers, and build awareness among them to mobilize enrolments from this group.
Based on inputs from UIDAI, review and finalize list of Introducers and notify the same in a public manner.
Introducers need to be enrolled in advance and have their Aadhaar numbers generated, registered and activated in Aadhaar database. Organize camps for enrolment of Introducers to ensure that all Introducers on the final list are enrolled into the program.
Introducer workshop is held to appraise them about their roles & responsibilities
Introducers are required to sign consent to being a Introducer which is stored by the Registrar. Introducer consent form format is provided by UIDAI.
Put in place systems to ensure ongoing monitoring of the Introducer list occurs at regular intervals. Based on performance, make changes/additions to the list as required and share with UIDAI. Ensure that both UIDAI and the Registrar have most up-to-date list of Introducers at all times.
Publicise the Introducer concept to make residents aware. Provide the resident information about acceptable Introducers. Publish list of Introducers and Verifiers at the enrolment centres along with their contact details. Detailed guidelines on Introducer selection, Introducers roles and liabilities are defined by UIDAI and published on UIDAI portal.

17. Identify and Deploy Verifiers

Registrar must appoint Verifiers for every centre.
Firm up Verification process. Shortlist the Verifiers and Registrar's supervisor. Schedule camps to educate verifiers.
The Registrar must ensure physical presence of verifiers during the operational hours of the enrolment centre and may appoint more than one Verifier in a center, if and where required.
The performance of Verifiers may be monitored by the Registrar.
The list of all Verifiers must be notified, by designation, by the Registrar before commencement of the enrolments and the list should be shared with the Regional office concerned.
They may be paid by the registrars out of the financial support provided by UIDAI to Registrars on successful Aadhaar generation. Roles and Responsibilities of Verifiers are defined by UIDAI.

18. Personnel for Grievance Redressal
The registrar is expected to put in place a Team that would serve to quickly address any matters requiring resolution that may pertain to the Registrar, but may be conveyed to the UIDAI Contact Centre. The Time taken for resolutions is to be finalized jointly.
Registrar should also identify an Officer to whom all relevant grievances may be forwarded and two senior officers for managing escalations of the same.

19. Print and Distribute Enrolment forms
Enrolment form is designed by UIDAI for capturing Aadhaar enrolment data.
Registrar can have a separate form for capturing KYR+ data.
Registrar needs to get the enrolment forms printed in sufficient quantities.
Registrar must ensure that the forms are available/ distributed free of cost at the enrolment centres.

20. **Data Transfer**

Finalise, with EA, Resident Data packets transfer modalities. Data can be transferred to UIDAI using online SFTP mode or through hard disks/memory sticks sent through suitable courier service.

Also define KYR+ and registrar data packet transfer mode and frequency.

21. **For Document Management**

UIDAI mandates storage of Enrolment form, PoI, PoA, DoB, PoR, and consent. These documents carry important and confidential resident information. UIDAI urges to handle enrolment documents with care and protect it from damage and theft. Registrar must do the following:

Identify whether the documents would be stored in hard copy/soft, scanned copy

Setup a mechanism for collecting and securely storing all the documents submitted by residents during enrolment till the UIDAI appointed DMS service provider collects document from registrar offices and provide receipt of the same.

Upon accumulation of specified batches of documents at one site, intimate UIDAI's DMS service provider for pickup of documents, handover documents and obtain sign off. Detailed process and guidelines of Document management and Registrar's role in same are published by UIDAI in Document Management Process.

If Registrar wants to store any additional documents, they may develop their own process for storing and managing those documents.

22. **Provide requisite data to Contact Centre**

The UIDAI has set up a Contact Centre for concern and issues that residents or UIDAI eco system partner may have in terms of enrolment, authentication and identity frauds etc. This contact centre serves as a single point of contact for the organization. Certain information is required by the contact centre, from the Registrar, related to enrolment exercise in their area. Registrars must furnish such details to the Contact centre to help effective functioning of the centre.

23. **Monitoring and Audits**

Registrar is responsible for Field level execution, monitoring and audit.

Audit enrolment centre readiness, EA processes and their effectiveness. It is recommended that Registrars setup a process to audit the performance of Enrolment Agencies and other partners they engage with.

Registrar must conduct sample audits in the entire gamut of enrolment process and data quality, training, logistics, grievance resolution and updation processes for controllership purposes.

Ensure IEC norms are being adhered to. Advise EAs to deploy IEC elements in a judicious and practical manner. Monitor the performance of Introducers and Verifiers.

The Registrar may also undertake appropriate measures such as monitoring of payment to operators' and supervisors' bank accounts, regular audits of EAs and enrolment centres, etc.

to prevent sub-contracting.
Randomly Review Acknowledgement and Consent data against PoI, PoA documents to ensure that data entered in the software is correct for each resident. In case any error is found in the data entered, inform the EA Supervisor and/or resident to initiate data correction.

24. **MIS**

Registrar must develop their own MIS systems for execution, monitoring and control. Registrar may help provide UID with reports/insights in significant issues as and when required by UIDAI.

25. **Data Protection and Security Guidelines for Registrars**

Registrars have a fiduciary responsibility and have to exercise a duty of care to secure and protect all the data (demographic and biometric) collected from the resident. UIDAI prescribes broad measures for data protection and security to be adopted by Registrars. Registrars must refer and abide by the same.

26. **Enforcement of UIDAI's suspension/debarment/dis-empanelment decisions**

UIDAI monitors the performance and data quality of Enrolment Agencies and their Operators and Supervisors on a continuous basis. UIDAI has formulated a suspension policy for non-compliant EAs and their Operators and Supervisors.

Registrar will be notified of the action where suspension/debarment/ dis-empanelment criteria are met. Registrars must get in touch with the UIDAI Regional Office and take immediate appropriate actions when intimated of such decisions.

27. **Enforcement of UIDAI's Returned Letters policy**

A report on returned letters will be shared by UIDAI with Registrars. Registrars must Review and investigate the various reason codes for Returned Letters. Where possible and required, Registrars may contact the Residents and educate residents on how to get in touch with contact center for their Letters. Registrars may involve/take help from India Post in investigations.

28. **Ensure UIDAI Exit Policy requirements are fulfilled**

If and when Registrar decides to exit the Aadhaar enrolment programme, they must fulfil requirements and sign necessary documents to meet the requirements of UIDAI's exit policy.

Verifier

Who is a Verifier?

For Verification based on Documents, the verifier present at the Enrolment Centre will verify the documents. Registrars must appoint personnel for the verification of documents. The services of the retired government officials who are generally well acquainted with such verification procedures should be utilized by the Registrars in case they are unable to spare serving officials for document verification. Any serving /retired official both from Government (including Armed forces and CPMFs) and PSUs including Banks not below the rank of Group 'C'/ class III employees may be allowed to be deployed as Verifiers. In the areas, like big cities and Metros, where registrar is unable to avail the services of such Retired/Serving government officials, services of an outsourced vendor can be availed of to provide verifiers with the approval from UIDAI Regional Office. The verifiers in an enrolment centre cannot be from the same vendor, hired as enrolment agency. Registrar needs to ensure that verifiers are appropriately trained before being put in the field.

The Registrar may appoint more than one Verifier in a centre, if and where required.

The list of all Verifiers must be notified, by designation, by the Registrar before commencement of the enrolments and the list should be shared with the Regional office concerned

What are the responsibilities of a Verifier?

For enrolment, Resident will bring his/her original documents along with the photocopy of the documents and filled Enrolment Form. Verifier must verify Photocopy of Documents and Enrolment Form details against original documents. Verifier also checks that the names of the documents captured in the enrolment form are correct and same as the original documents produced by the resident.

Verifier needs to be available in the enrolment center throughout the operating hours of the center. Registrars should ensure physical presence of verifiers during the enrolment.

It is verifier's responsibility to ensure that Enrolment form is filled completely and correctly as per UIDAI enrolment process. No mandatory field should be left blank and resident should be encouraged to fill optional fields like mobile number and email address. Verifier will sign and stamp the Enrolment Form after verification. If stamp is not available, the verifier can sign and put his/her Name. The resident will then go to the Enrolment Agency Operator for getting enrolled.

However, if the resident is enrolled and has come for Correction for a particular demographic

field, the resident need not enter all details in the Form. The resident must provide his/her original Enrolment Number, Date and Time (together known as EID), his/her Name and the field which needs correction. Verifier will only verify if it is one of the fields requiring verification of documents. Verifier will use the same UIDAI verification guidelines as used during resident enrolment.

Where hard copy of documents is being stored, the photocopy of documents may also be verified with Verifiers signature/thumb print and stamp/Name, except in case where copies attested / certified by a public notary / gazetted officer are being submitted.

The Verifier is physically present at the enrolment centre every day and, thus, can monitor the Enrolment Centre performance and provide immediate information to UIDAI and Registrar on process deviations and malpractices at the enrolment centre.

What are the UIDAI Guidelines for Verification that the Verifier must keep in mind while verifying the Documents?

Verification guidelines are listed below:
1. Make sure that the resident has original documents for verification. In instances where original documents are not available, copies attested / certified by a public notary / gazetted officer will be accepted.
2. The documents produced by the resident for Aadhaar enrolment must be in the list of approved documents. List of UIDAI approved Proof of Identity (PoI), Date of Birth (DoB) , Proof of Address (PoA) and Proof of Relationship (PoR) documents is available on http://www.uidai.gov.in/images/FrontPageUpdates/valid_documents_list.pdf

UIDAI and Registrars shall have the authority to amend and enlarge the list of valid documents as and when necessary.

3. A specimen for letter of certification is attached in Annexure 1. This format is for certification issued by officials/ institutions (only those that are recognised in the UIDAI's valid list of documents) for Proof of Identity and Address.
4. Verifier can refuse verification, if they suspect forged/altered documents. In cases where Verifier refuses verification of the documents produced, reasons should be recorded in brief by the Verifier on the Enrolment Form. In case the Verifier refuses verification with reasons or turns the resident back without recording any reasons, the resident can approach a designated authority/cell created by the Registrar at the Block level for redressal of grievances.
5. Verify Name, Date of Birth, Address, and Relationship Details against PoI, DoB, PoA, PoR, respectively.

6. Name
o PoI requires a document containing the resident's name and photograph. Verify that

document has both.
o If any of the PoI document submitted does not contain the photograph of the resident, then it will not be accepted as a valid PoI. In order to be inclusive and free of harassment, documents with older photographs are acceptable.
o Confirm the name in the document by asking the resident his/her name. This is to ensure that the resident is providing own documents.
o The name of the person should be entered in full. It should not include salutations or titles like Mr., Miss, Mrs., Major, Retd. etc
o It is very important to write the person's name very carefully and correctly. For example, the respondent may tell that his name is V. Vijayan whereas his full name may be Venkatraman Vijayan and similarly R. K. Srivastava's full name may actually be Ramesh Kumar Srivastava. Similarly, a female enrollee may tell her name as K. S. K. Durga while her full name may be Kalluri Surya Kanaka Durga. Ascertain from her/him the expansion of her/his initials and check the same in the documentary evidence produced.
o In case of difference in the name declared and the one in document (PoI) is limited to spelling and/or sequence of first, middle and last name, the name as declared by the resident may be recorded.
o If two documentary proofs produced by the enrollee have variation in the same name (i.e., with initials and full name), the enrollee's full name should be recorded.
o Sometimes the infants and children may not have been named yet. Try to ascertain the intended name for the child by explaining to the enrollee the importance of capturing the name of the individual for allotting UID. In case of non availability of supporting documents for PoI, the name should be recorded with the assistance of the Introducer.

7. **Date of Birth** (DoB)
o Date of birth of Resident must indicate day, month and year in the relevant field.
o If the Resident provides documentary evidence of Date of Birth, then the Date of Birth is considered as "Verified". When resident declares the DoB without any documentary evidence, then date of birth is considered as "Declared".
o When the resident is unable to give exact date of birth and only age is mentioned by the resident or approximated by the verifier then only age is recorded. The software will automatically calculate year of birth in such case.
o The Verifier should check the entry in the enrolment form and ensure that the resident has correctly indicated the date of birth as "verified"/"declared" or has filled his/her Age.

8. **Residential Address:**
o Verify that the PoA contains the name and address. The Verifier should ensure that the name in the PoA document matches with the name in the PoI document. A difference in the name in PoI and PoA document is acceptable if the difference is only in spelling and/or sequence of first, middle and last name.
o The "care of" person's name, if any, is usually captured for children and old age people living with parents and children, respectively. If not available, one can leave this Address line blank.
o Enhancement of address is allowed. The resident may be allowed to add minor fields such as House No., Lane No., Street Name, correcting typographic errors, minor changes/ corrections to pin code etc. to the address listed in the PoA as long as these additions/modifications do not alter the base address mentioned in the PoA document. If the changes requested are substantial and change the base address that is listed in the PoA, the

resident will be required to produce an alternate PoA or enroll through an Introducer.

9. **Relationship Details:**
o In the case of children below 5 years, "Name" and "EID/UID" of one of the parents or guardian is mandatory. Parent/Guardian must produce their Acknowledgement/UID letter when enrolling children (or they can be enrolled together). Parent/Guardian's Name and EID/UID should be verified.
o In the case of an adult, no verification will be done for the information on parent or spouse. They are recorded for internal purposes only.

10. **Head of Family(HoF):**
o Verify that the PoR document establishes relation between the Head of Family and the family member. Only those family members can be enrolled based on the relationship document (PoR), whose names are recorded on relationship document.
o Head of Family must always accompany the family member when the family member is getting enrolled.
o The verifier must also check the HoF details in the Enrolment Form in case of HoF based verification. HoF's Name and EID/UID in form should be verified against the Acknowledgement/Aadhaar letter.
o Ensure that in case of HoF based enrolments, the relationship details are also of the HoF only.

11. **Mobile Number, Email address:**
If the enrollee possesses and is willing to provide his/her Mobile Number and / or Email Address, these optional fields must be filled in. Verifier can inform the importance of these fields to the resident. UIDAI can get in touch with the resident using this information, if required, like in case of returned letters.

Introducer

How are Residents without documents enrolled in Aadhaar?

Key demographic data needs to be verified properly at the time of enrolment. Residents can bring any of the approved documents as Proof of Identity (PoI) and Proof of Address (PoA). If a resident is unable to provide documentary proof of identity or proof of address, they can be enrolled through a pre-designated "Introducer" who is identified and notified by the Registrar or Regional Offices.

An Introducer is a person who is authorized by the Registrar to introduce a resident who does

not possess any PoA/PoI documents. This introduction does not tantamount to giving a character certificate to resident.

Who is an Introducer?

Introducers are individuals (for example, Registrar's employees, elected local body members, members of local administrative bodies, postmen, influencers such as teachers, health workers & doctors, Aanganwadi / ASHA workers, representative of local NGO's etc.) identified by a Registrar and registered in UIDAI's CIDR as "Introducers". In certain cases, the UIDAI Regional Office may itself take the initiative to identify a pool of Introducers for the convenience of the Registrars.

Introducer must be above the age of 18 years and Introducer must not have a criminal record.

Introducers will be linked to a Registrar. The same Introducer may be used by more than one Registrar as long as they are identified by the concerned Registrar and registered in UIDAI's CIDR as "Introducers" for the particular Registrar. Therefore, the Introducer can only introduce people within the Registrar's jurisdiction. In addition, a Registrar can further limit the operations of an Introducer by administrative boundaries (State, district level).

What are the Responsibilities of an Introducer?

Once the Registrar identifies introducers region-wise (District/State in which the Introducer is authorized to work), he will notify the Introducers. The Introducers must:

1. Attend the Aadhaar awareness workshop organized by the Registrar and UIDAI to acquaint them with the Aadhaar program and understand Introducer responsibilities and liabilities.
2. If the identified Introducer is ready to work as an Introducer, he/she will have to give a written consent (prescribed Performa attached as annexure) to being an Introducer for the purpose of enabling Aadhaar enrolments and to follow the guidelines and procedures laid down for the Introducers by the Unique Identification Authority of India (UIDAI) and the Registrar
3. Introducers need to be enrolled and must have received their Aadhaar numbers and signed the consent forms before they start introducing residents in the field.
4. They must ensure that the Registrar has registered and activated them as an Introducer at UIDAI.
5. Introducers must keep themselves informed on the Enrolment Schedules, Enrolment Centre locations and operational hours of the Enrolment Centers in their assigned territory.
6. They must ensure that their contact information is correctly displayed at the Enrolment Centre. In case of no display/incorrect information, ask the Enrolment Centre supervisor to display/correct the details.
7. Introducer must be easily accessible to the residents.
8. The Introducers must check the Resident's Name and Address on the enrolment form for

correctness and completeness. Introducer should also check his/her own details in the form and then provide his/her signature/thumbprint on the Enrolment Form space provided.
9. Introducers should make themselves available during the working hours of the EC for endorsing residents. In case, they are not available during the operational hours, they can visit the Enrolment Centre at the End of the Day and check the list of residents pending for their endorsement.
10. Introducer must carefully check the Name and Address details of the Resident and provide their Approval/Rejection.
11. Introducer has to provide their biometric on Aadhaar client to endorse a resident's enrolment.
12. The Introducer also signs/provide thumbprint on the consent for enrolment where consent print requires the same.
13. Introducer confirms the identity and address of the resident they are introducing
14. Introducer must only introduce residents who do not have documentary proof of identity or address
15. Introducer is not obliged to introduce every person who approaches them
16. Introducer cannot charge fees for introducing residents. However, Registrars can prescribe an honorarium to them for this work.

What are the Liabilities of an Introducer?

Introducer's liabilities:

1. Introducer must not collude with a person to impersonate another person (dead or alive) at the time of enrolment.
2. Introducer must not help an Aadhaar holder to deliberately take on the identity of another person by changing their demographic information or even collude to provide false biometric information.
3. Strict action will be taken against the Introducer for violation of guidelines.

Enrolment Agency

Who is an Enrolment Agency (EA)?

Enrolment Agencies are entities hired by the Registrars for undertaking demographic and biometric data collection for UID enrolment. Enrolment Agencies must ensure continued empanelment by UIDAI in order to be engaged by Registrars. If non-empanelled agencies are engaged by Registrars, they are also subject to the same terms and conditions as the empanelled agencies.

Are EAs allowed to sub-contract Enrolment Work?

Sub-Contracting of Enrolment Work is not allowed for private/ commercial Organizations/PSUs /Govt. Companies /Autonomous bodies. However, field level manpower such as enrolment operators and supervisors can be hired through third parties. EAs must provide details of the companies from which they are going to hire this manpower. However, Government Organizations may choose to franchise enrolment work to CSCs/ Local Government bodies.

What are the Preparatory Activities that an EA must do prior to starting enrolments?

Preparatory Stage Activities of an EA

EA must identify their Project & Technology managers who will be part of the Joint Working Group headed by the Head of the Nodal/Registrar Department. Initiation and On-boarding Workshop for EA must organised by Registrar and UIDAI will provide detailed enrolment process & implementation overview. EA must familiarize themselves with Enrolment process and policies including periodic amendments/updates. The scope of work of the Enrolling Agency (EA) includes the following activities:

1. **Procure enrolment hardware, software including Biometric Devices as per UIDAI Specifications** The enrolling agency should procure enrolment hardware, software including certified biometric devices (for fingerprint and iris capture), used for capture of biometric data at the enrolling station, which conform to UIDAI specifications. EA must procure only those Biometric Devices that are certified by UIDAI or its duly authorized agency. The EAs must also ensure continued technical support by the suppliers for the hardware.

2. **Hire & Train Manpower for Enrolment**

The Enrolling Agency shall hire manpower, Operators and Supervisors, to operate the enrolment station/centre as per the guidelines prescribed by UIDAI. The enrolling agency must have Technical personnel to provide technical support during enrolment at the enrolment centres. Technical personnel for attending power /system / biometric instrument related maintenance problems should be available on call in a centrally located place covering about six enrolment centres so that the downtime can be minimized.
EA must make sure that the Operators and Supervisors are of age 18 years and above. The Operator should be minimum 10+2 pass and should be comfortable using computer. The Supervisor should be minimum 10+2 pass and preferably a Graduate and should have a good understanding and experience in using a computer.
EA must ensure compliance to Labour laws and all statutory provisions in various Labour regulations that is PF, ESI, Industrial Disputes Act, Contract Labour Act and Minimum Wages Act etc.

The personnel should be given mandatory induction training on the various activities and equipment and gadgets involved/used in the enrolment process and resident enrolment, transliteration skills in local language, to enable them to understand and adjust to the local situation. The mandatory induction training shall be compulsory before deployment of the personnel. The EA will inform concerned RO Regional Offices of UIDAI prior to training schedule and will also give a follow-up report.
The enrolment agency shall ensure the availability of the requisite infrastructure for imparting training as per UIDAI guidelines
The Operators and Supervisors should have obtained certificate from a testing and certifying agency authorized by UIDAI. Ensure correct certification as per specific roles. A certified Operator cannot work as a Supervisor.
Payments to operators and supervisors should be made preferably to their bank accounts.

3. Enrol Operator/Supervisors and Register and Activate them at UIDAI

Operator /Supervisors must have their Aadhaar numbers generated and certification test passed for getting activated in accordance with UIDAI guidelines prior to commencing enrolments. Do not deploy them for enrolment without the fulfilment of these mandatory requirements.
EA admin user must use unique user IDs for activating their Operator/ Supervisors. Do not use one password for multiple set of Operator IDs. Ensure all details entered are correct on UIDAI technology portal and certification agency's portal and there is no mismatch.
EA must ensure availability of manpower activated in accordance with Aadhaar guidelines prior to commencing enrolments.
EAs will have to demonstrate that they have certified the active operators, requisite machines and hardware available to be deployed. EAs will have to declare enrolment station deployment plans i.e. when and where the centers will be established. EAs will also demonstrate that they have the requisite supervision infrastructure available. Based on this information, ROs will assess the preparedness of the Registrars and EAs and may then allow the on-boarding of stations.

4. Get established as an Enrolment Agency at UIDAI
The EA must receive their EA code from UIDAI
The EA must ask the Registrar to establish the link between them (Attach EA) at UIDAI
Receive admin password for portal and auth code for client registration from UIDAI
Obtain SFTP account setup and password

5. Ensure that Pin code data for planned enrolment locations is checked in Pin Master of Aadhaar software, and is correct and complete. Review and Report missing/incorrect Pin codes and use Pin code correction process for getting the Pin Numbers corrected.

6. Software Installation, Configuration and Registration
The latest version of Aadhaar Enrolment software client needs to be installed, configured and registered with CIDR. The Enrolment Agency needs Auth User and Auth Code from UIDAI technology team to register its clients.
The person performing the system configuration is typically a representative of the Registrar. Normally the Registrar may ask the EA to perform the installation and configuration. In such a case, the configuration and registration may be done in presence of Registrar's representatives.

Load and test Pre-enrolment data on enrolment centre laptops / desktops and ensure it is accessible / searchable.
All latest Master Data such as Pin code, Operator credentials, list of documents etc. should be loaded on client
Thorough testing of Aadhaar client working in integration with pre-enrolment data and KYR+ applications, along with local language support, pin code and master data availability
Ensure all Registered stations are active at UIDAI
Ensure Operator/Supervisor/Introducer (OSI) are on boarded on the enrolment stations

7. EA must ensure with Registrar that **Aadhaar and KYR+ Enrolment Forms** are printed, ready for distribution/distributed to residents. If enrolment forms are distributed and filled in advance, it will help speed up enrolment at the Centre. The enrolment forms can be used as a tool for crowd management by controlled distribution.

The print and paper quality of forms should be ensured as the forms will be stored as per Document Management System.

8. **Setting up of Enrolment Centre(EC) and Enrolment Stations (ES)**
EA will assist Registrar in developing enrolment schedules. EA will work with the Registrar in identification of suitable enrolment centres at scheduled locations. Once EC are identified, EA must ensure readiness of the EC as per the latest Enrolment Centre Setup Checklist (Annexure 1). The Enrolment Centre Setup Checklist by UIDAI enlists the various requirements at Enrolment Centre and Station level and is to facilitate the EA in planning.
Ensure adequate stationary like paper for printing and other logistics are available at centre
Ensure adequate power and other backup arrangement at enrolment centre
Deploy Hardware, Software for Enrolment. Working of all equipment and application at every station must be tested.
EA must not undertake enrolment operations at locations without valid agreement with the Registrars.
The Enrolment Agencies also need to fill the Enrolment Centre details at UIDAI portal.
EA must adhere to Safety Procedures, Rules, Regulations, & Restrictions and shall comply with the provisions of all laws including safety and labour laws, rules, regulations and notifications issued there under from time to time. EA shall take all measures necessary or proper to protect the personnel and facilities and shall observe all reasonable safety rules and instructions.

9. **Contact Centre information filled**

EA must fill the forms with information required by UIDAI Contact Centre and submit. This information pertains to EA contacts at EC, Enrolment Centre address and working hours etc.

10. **Help Create Awareness**

Enrolment Agency needs to work with the Registrar in communication and generating resident awareness at grass root level. Prior to the commencement of the Enrolment operations the Enrolment Agency shall work closely with the local governing bodies, key introducers in publicizing the Aadhaar, its importance and schedule for Aadhaar registration in that location. EA must prominently display important information relating to consent and operator responsibilities inside the enrolment centres.

The role of the enrolment agency should be limited to publicising the content provided by the UIDAI/ Registrars. The EA should not add to / modify /delete the content provided by Registrar/ UIDAI.

What are the Activities that an EA performs during Enrolment Stage?

Enrolment Stage Activities of an EA

1. Capture Demographic and Biometric Data

The enrolment agencies will use the latest client software prepared and released by UIDAI for the collection of demographic and biometric data from time to time as per standard processes specified by UIDAI. The acknowledgement should be provided to the resident and resident's consent taken at the end of enrolment without fail. Ensure End of Day Review of data packets by Supervisor. All UIDAI defined processes are available on the UIDAI portal. EA must ensure facilitation for good quality data capture at the enrolment stations.

2. Data Transfer to UIDAI

The data collected at the time of enrolment will be transferred to UIDAI for storage and processing in Central Identities Data Repository (CIDR) as per the prescribed format as per the UIDAI recommended processes. EAs can transfer data to CIDR either by sending memory stick/hard disks or through SFTP mode. The EA must export and upload data at the most within 20 days of enrolment. The client will freeze if packet pending for uploads exceed 1000 numbers on the station. Similarly workout the transfer of Registrar packets with the Registrar and hand them over as per agreed process and guidelines.

3. Sync and Data Backup

The enrolment client, after successful enrolments, needs to be synched up with the server every 10 days, mandatorily. The synch process requires network connectivity.

EA must take back-up of data captured, at least twice a day, and retain it for a period of minimum 60 days (or as specified by UIDAI from time to time).

4. Privacy & Security

Enrolment agencies are responsible to make sure that the data is kept in a very secure and confidential manner and under no circumstances, shall they either use the data themselves or part with the data to any other agency other than the UIDAI or the Registrar. Mechanisms to ensure the same have to be put in place by the Enrolling agency and shall be subject to audit by UIDAI/its representative from time to time. The EAs must familiarize themselves and strictly adhere and comply with the data security guidelines issued by UIDAI from time to time. If there is any violation of privacy by the enrolling agency or through its employees,

contractual or otherwise, it shall be construed as a breach of contract, apart from attracting the penal provisions of the Act which will govern the operations of the Authority. If Registrar has prescribed any security and privacy policies/guidelines, then those must be adhered to in addition to UIDAI guidelines.

5. Provide Electronic MIS Reports on Enrolment Status

Enrolment Agencies will be required to send statistics on enrolment status to Registrar/UIDAI as prescribed by them from time to time.

6. Document Management System

The Enrolment Agencies are expected to collect Hard Copies/Scan documents, consent and enrolment forms from the residents. Records must be indexed and stored in such a way that they are retrievable, accessible and safeguarded against environmental damage till the time they are submitted to Registrar/UIDAI. The enrolment agency must maintain a list of the documents collected and submitted, for the purpose of reconciliation and future reference. The guidelines related to Document Management System have been published by UIDAI.

As and when Scanning policy comes in place, EA will have to change over from maintaining hard copy of documents to managing documents in scanned form.

7. Crowd Management

EA must put in practice mechanisms like token system to manage crowd at the enrolment centre and to avoid prolonged wait by resident.
EA staff must wear uniform or distinguishing garment/s at enrolment centre so that if residents need help they can easily identify employees by their attire.
All field operators deployed for collecting pre-enrolment data must carry identity cards.
Display Name, Code, and contact number of EA Supervisor at enrolment centres
EAs can use online appointment system in consultation with Registrar and RO.
EA must ensure that the Operators and Supervisors are polite and courteous with the residents.

What activities other than those listed in preparatory activities and enrolment must an EA take on an on-going basis?

On-going Activities of an EA

1. EAs performance must be continuously assessed during the execution of project/assignment and appropriate action taken in accordance with the policy in place at that time.

EA must co-operate with the audit party of UIDAI/Registrars/auditing agencies empanelled/ appointed by them.

2. EA must take remedial / corrective action in case of process / quality deviations.
3. EA must have a mechanism for Grievance Redressal and also an escalation matrix defined for addressing issues from field/UIDAI/Registrar.
4. EA must maintain credentials of Operators, Supervisors and Enrolment Stations and keep updating active Operator, Supervisor, Station details at UIDAI
5. EA consortium must observe highest standards of ethics during the execution of the awarded contracts for Aadhaar enrolment.
6. Any work, as and when required, for smooth and timely execution of project may be supported by the EA.

Operator

Who is an Operator and what are his/her qualifications?

An Operator is employed by an Enrolment Agency to execute enrolment at the enrolment stations. To qualify for this role, person should satisfy the following criteria:

1. The person should be of age 18 years and above.
2. The person shall be minimum 10+2 pass.
3. The person should have a basic understanding of operating a computer and should be comfortable with local language keyboard and transliteration.

Before starting work as an Operator:

1. The Operator should have been enrolled for Aadhaar and his/her Aadhaar number should have been generated.
2. The Operator should have undergone training on the process of UID Enrolment and various equipment and devices used during Aadhaar enrolment. Organising this training is the responsibility of the EA.
3. The Operator should have obtained certificate from a testing and certifying agency authorized by UIDAI.
4. For certification, Operator needs to register with UIDAI appointed certification agency for taking test at a suitable time and test centre location
5. Operator must ensure that the Name and EID/UID provided during registration for test is same as that entered during Aadhaar Enrolment
6. The Operator should have been activated, in accordance with UIDAI guidelines, prior to commencing enrolments. The Enrolment Agency is required to have a unique Operator ID for each, to activate them.

What are the Ten Commandments that an Operator must remember during Resident Enrolment?

At the Enrolment Centre, Operator's role is to capture Demographic and Biometric data of the resident getting enrolled. When performing his/her role as an Operator at an Aadhaar Enrolment Centre ensure the following **"Ten Commandments":**

1. Operator must first get on-boarded by providing his/her own biometrics in the Aadhaar client software. On-board (Enrolled) User means user's biometric details verification at UIDAI is successfully completed and stored in local database at the enrolment station.
2. Make sure to Login with your own Operator ID in Aadhaar client, for undertaking enrolments, and log off the application when going away from the seat so that no one else can use your login window for enrolments.
3. Every time on login, Operator must make sure that the date and time setting on the computer is current.
4. Make sure that the station layout is convenient for you as well as the Resident. The preferred layout is shown in the Resident Enrolment Process Document. Brief the enrolment process to resident before and during enrolment to put the resident at ease and facilitate data capture
5. When the resident comes for enrolment, first make sure from the photo on documents that they belong to the same resident whose enrolment is to be done. Confirm that the form and documents belong to the same resident who is getting enrolled.
6. Check that the resident's enrolment form is verified and carries Verifier's signature/thumb print and stamp/initials. The form must also carry Resident's (Applicant's) signature/thumbprint.
7. In case of Introducer/HoF based enrolment, the Introducer/HoF's signature/thumbprint should be available in the form along with their details filled in the fields provided for Introducer and HoF, respectively.
8. Capture demographic and biometric data of the resident in the Aadhaar client software. The Operator must ensure to follow the sequence of data capture as per the screens provided on the software client.
9. Make sure that the resident's screen is on all the time during the enrolment and ask the resident to cross check the data being entered and review demographic data with resident before signing off.
10. Print, sign and provide acknowledgement to the resident and take resident's signature on consent at the end of enrolment.

What are the UIDAI Guidelines for Demographic Data Capture?

Demographic Data Capture Guidelines:

a. Enter the demographic details of the resident from the verified enrolment form.
b. Enter all the data in the Aadhaar software as provided in enrolment form. Even the non-mandatory fields like mobile number and email ID are important. UIDAI can get in touch with the resident using these details, if required, like in case of returned letters. Thus do not leave these fields blank where resident has provided this information. Similarly information sharing and banking consents should be carefully filled in the software client as per the enrolment form.
c. If using Pre-enrolment data, the Operator will retrieve resident's demographic details using pre-enrolment ID. Make sure that the data pulled using pre-enrolment ID belongs to the resident getting enrolled, by confirming against enrolment form details. Do not limit the check to Name only and quickly confirm other details also like gender, age etc to make sure.
d. Check and correct the pre-enrolment data as per verified enrolment form details. There can be errors in spelling, transliteration and completeness of pre-enrolment data that need correction.
e. Pay attention to Data Aesthetics during demographic data capture. Avoid improper use of spaces, punctuation marks, capital & small letters during data capture.
f. Leave those non-mandatory fields blank where no data is provided by resident. Do not enter N/A, NA etc. in fields where Resident has not provided any data.
g. Filling Father / Mother / Husband / Wife / Guardian field is not mandatory for residents above the age of 5 years in case the adult is not in a position or does not want to disclose. Then select checkbox "Not Given" in "Relationship to Resident".
h. In case of children below the age of 5 years one of the parents' or guardian's name shall be recorded and UID or Enrolment ID (either of the two numbers) shall be recorded. This is mandatory.
i. It is not compulsory for only father's name to be recorded against the 'parent's name.' Mother's name can alone be recorded for the 'parent's guardian's' name if so desired by the parent.
j. Enrolment of the parent is mandatory prior to the child. If the child's father /mother / guardian has not enrolled or does not possess UID at the time of enrolment, the enrolment of that child cannot be done.
k. For Head of Family (HoF) based verification Name, EID/UID of HoF and Relationship Details of the family member to HoF are mandatory details to be entered.
l. Once Demographic Data is entered, Operator will capture the Biometric data of the resident.

What are the UIDAI Guidelines for Biometric Data Capture?

Biometric Data Capture Guidelines:

a. Check resident's eyes and fingers for fitness (missing/amputated). If the resident has any deformities due to which it is not possible to take fingerprints/iris, these also have to be captured as a biometric exception.
b. Check and indicate Biometric Exceptions in the software, only where applicable. Do not mark biometric exceptions where biometrics can be captured. It will be treated as 'fraud' and invite strictest penalty.
c. In case of Biometric exception, always take the Exception photograph of the resident showing resident's face and both hands, irrespective of the type of exception.

d. The enrolee may not be in a position to keep herself / himself in correct posture for reaching biometric instruments or for photograph due to old age or sickness. In such cases the operator should arrange to take the biometric data by moving the equipment close to the enrolee.
e. If the finger/iris of the resident has a temporary damage and it is not possible to capture the biometric, the Operator will record it in exceptions. The resident should later get his/her biometric updated.
f. Capture Biometrics - Facial Image, IRIS and Fingerprints.

1. **Guidelines for Facial Image Capture**
a. **Enrollee Position:** For capturing facial image, it is advisable for the operator to adjust the camera instead of the Enrollee to position herself/himself at the right distance or in the right posture. Frontal pose needs to be captured i.e. no head rotation or tilt. The resident should be instructed to be seated properly with their back upright and their face towards the camera.
b. **Focus:** The capture device should use auto focus and auto-capture functions. The output image should not suffer from motion blur, over or under exposure, unnatural colored lighting, and distortion.
c. **Expression:** Expression strongly affects the performance of automatic face recognition and also affects accurate visual inspection by humans. It is strongly recommended that the face should be captured with neutral (non-smiling) expression, teeth closed, and both eyes open and looking into the camera.
d. **Illumination:** Poor illumination has a high impact on the performance of face recognition. Proper and equally distributed lighting mechanism should be used such that there are no shadows over the face, no shadows in eye sockets, and no hot spots. No light exactly above the enrollee should be used since it can cause shadows. Light should be diffused and placed in front of the enrollee so that there are no shadows under the eye.
e. **Eye Glasses:** If the person normally wears glasses, it is recommended that the photograph be taken with glasses. However, the glasses should be clear and transparent. Dark glasses /tinted glasses should be taken off before taking the photograph.
f. **Accessories:** Use of accessories that cover any region of the face is not permitted. For example, women in purdah would have to reveal the full face before the photograph is taken. Similarly women in Ghoonghat would have to clearly reveal the full face before the photograph can be captured. The head may remain covered but the full face contour should be visible.
g. Further, accessories like turban/head gear are also allowed as religious/ traditional practices.
h. However, accessories like eye patches are allowed due to medical reasons. This would also mean an exception needs to be recorded for Iris, because only one Iris can be captured.
i. Operators need to be trained to obtain the best possible face images that satisfy requirements. Even if the quality flag is green but the Operator is able to judge that a better picture can be taken, then same should be attempted. However, it should be borne in mind that recapture should not become harassment for the resident.
j. For children, it is acceptable that the child sits on parent's laps, but it needs to be ensured that parent's face is not captured along with child's face. The background may get rejected due to non white screen in case of children but two faces should not get captured in one picture.

k. Actionable feedback needs to be checked for captures that fail. Some of the actionable feedbacks in software are:

- No face Found
- Enrolee too far
- Enrolee too close (eye distance in input image is greater than one third of image width)
- Pose (Look Straight)
- Insufficient lighting
- Very low face confidence (faceness, object not identified as human face)
- Non-uniform lighting (of face in output image)
- Incorrect background (in output image)
- Insufficient lighting (bad gray values in face area of output image)

l. If any biometric exceptions have been specified on the demographic screen, these should be captured as photographs on the Photograph screen.
m. Only facial image is captured for children below 5 years. Iris and fingerprint screens will not get activated for children below 5 years

2. **Guidelines for Capturing Fingerprints**

a. The images of all the ten fingers are to be captured. The fingerprints must be captured in the sequence of slaps of four fingers of left hand, right hand followed by the two thumbs.
b. The fingers have to be positioned correctly on the platen to enable capture. There should be no direct light shining on the platen. Use the Indicators on fingerprint devices for positioning of fingers. The fingers should be placed in right direction on the device. Please consult the manufacturer manual incase of any doubt or else consult the supervisor.
c. Use a lint free cloth periodically to clean the platen of the finger print device for good finger print capture
d. Check devices periodically for scratches, out of focus images, only partial images getting captured. In case any such problem is noticed, then report to your Supervisor/HQ and request for change of equipment.
e. Fingerprints cut off, wet/smudged fingerprint; very light prints due to insufficient pressure will result in poor quality. The resident's hands should be clean (no mud, oil etc.). Ask resident to wash hands with water and soap, if necessary.
f. The fingers should not be excessively dry or wet. Moisten with a wet cloth or dry finger with a dry cloth
g. The Enrollee should be requested to place all four fingers of the left hand/right hand/two thumbs to platen of the fingerprint scanner for the four-finger capture to ensure good contact and maximize the area of the captured fingerprints. Ensure that the fingers are placed flat and till the top joint of the finger is placed well on the scanner. The top of the fingers should be within the platen area and not outside the defined area.
h. If automatic capture does not happen, the operator should force the capture when force capture tab is enabled in the enrolment software.
i. The operator should check the actionable feedback when capture fails. Some actionable feedbacks provided by software are:

- Number of fingers present does not match with expected number of fingers
- Finger not positioned correctly
- Too much Pressure (duty cycle)
- Too little pressure
- Central region missing
- Excessive moisture (wetness)
- Excessive dryness

j. The operator should visually check the image for quality and for typical problems. In case there are problems go back to steps above to retry the capture.
k. When image quality is pass or if maximum number of captures are exhausted , move on to the next step.
l. Fingerprints are best captured in standing position
m. In case of additional fingers, ignore the additional finger and capture the main five fingers.
n. Make sure your own fingerprints do not get mixed with the resident's fingerprints. Operators can carefully put small pressure on the resident's fingers to capture the fingerprints but always make sure not to mix your own fingerprints.

3. Guidelines for Capturing Iris

a. The operator and not the Enrollee will handle the capture device, generally.
b. Children can be told that it is like taking photos/pictures so that they are not apprehensive.
c. The Enrollee will be required to sit in a fixed position, like taking a portrait photograph.
d. The software is able to measure the iris image quality. An initial image quality assessment would be done to provide feedback to the operator during the capture process. The software alerts the operator with actionable feedbacks, if the captured iris image is of insufficient quality. Some actionable feedbacks provided by software are:

e. Occlusion(significant part of iris is not visible)
- Iris not in focus
- Gaze incorrect(resident looking away)
- Pupil dilation

f. The iris capture process is sensitive to ambient light. No direct or artificial light should directly reflect off Enrollee's eyes.
g. The device should be held steady. Incase device requires to be held by resident, the enrolment operator/supervisor may help the resident to hold the device steady.
h. Table light used for facial image capture should be switched off during iris capture. Direct sunlight or any other bright light shining on resident's eye will create reflections and result in poor quality image.
i. Operator must instruct the resident to look straight into the camera, open eyes wide open (one easy way to do this is to ask the resident look angry or stare) and do not blink during iris capture. Resident has to be stationary.
j. If resident is experiencing difficulty during Iris scan and recapture is required, then the operator may navigate to next screen to capture other details and then return to Iris capture. This will relax the resident from constant pressure to keep eyes wide open during iris capture.
k. The Operator needs to be patient during capture and wait for the device response instead of scrolling, navigating back and forth on screen.

How does the Operator Review Data with the Resident?

The Operator must show the data entered to the resident on a monitor facing the resident and if required, read out the content to the enrollee, to ensure that all details captured are correct. During Review of the enrolment data with resident, Operator must read out critical fields to

the resident before the Operator Finishes the Enrolment.

a. The Operator must reconfirm the following fields:
Spellings of Resident's Name
Correct Gender
Correct Age/Date of Birth
Address – Pin Code; Building; Village/ Town /City; District; State
Relationship Details – Parent/Spouse/Guardian ; Relative Name
Accuracy and Clarity of Photograph of the resident
b. In case of any errors, Operator must correct recorded data and review again with the resident. If no corrections are required, resident will approve the data.

What Does the Operator do after Capturing Demographic and Biometric Data of the Resident?

a. The Operator will then provide own Fingerprint to sign-off the data captured for the resident. Make sure that the fingerprint given is good quality. Use the Indicators on fingerprint devices for positioning of fingers. The fingers should be placed in right direction on the device.
b. Do not allow anyone else to sign for an enrolment that you have done. Do not sign for enrolments done by others.
c. Operator will get the Supervisor to Sign Off in case enrollee has biometric exceptions
d. In case the verification type is selected as Introducer/HOF, get the Introducer/HOF to sign off on the review screen.
e. If the Introducer is not physically present at the time of enrolment select the check box "Attach later" so that the enrolment can be verified by the Introducer at the End of the Day.
f. Operator can select the language in which the legal/declaration text on print receipt shall be printed on consent.
g. Operator must ask the resident his/her preferred language in which the receipt must be printed. On selection of any of the declaration language option, the print receipt will be printed in the selected language i.e. English or any local language set on the configuration screen.
h. Take Resident's signature on consent and file the same along with resident's other documents. The Resident's consents are important as they are resident's approval/disapproval, to the UIDAI, sharing his/ her information with agencies engaged in delivery of welfare services and opening/linking of Aadhaar enabled bank account.
i. Sign and Provide Acknowledgement to resident. The acknowledgement is a written confirmation of the resident getting enrolled. It is important for the resident as it carries the enrolment number, date and time that the resident will need to quote when interacting with UIDAI and its Contact Center for information on his/her Aadhaar status. The enrolment number, date and time are also required if any correction in the resident's data is required to be done using Correction process. Thus the operator must make sure that the acknowledgement and consent printed is clear and legible.
j. While handing over the acknowledgement to the Resident, the Operator must inform below to the resident

- The Enrolment Number printed on acknowledgement is not the Aadhaar number and that the Resident's Aadhaar number will be communicated through a letter subsequently. This message is also printed in acknowledgement.
- The resident must preserve his/her and the children's Enrolment Acknowledgement Slip for future reference.
- In case of introducer based enrolment, the introducer will have to properly sign off within the specified period and Resident's Aadhaar is subject to endorsement by a valid Introducer.
- There is a 96 hour period during which the resident's data correction, so in case of any mistake they should avail this facility.
- To know the Aadhaar Generation Status they can call the Call Centre or log on to e-Aadhaar portal/Aadhaar Portal/website.
- Aadhaar number will be delivered by the local post office/or other designated agency in the address provided at the time of enrolment.

What are the Document Management Guidelines of UIDAI?

Maintaining Document Hard Copies

a. Where hard copies of documents are being stored, the Operator will collect the following documents from the resident:

- Filled and Verified Enrolment Form – for each enrolment
- Copy of Proof of Identity (PoI)– for document based enrolment
- Copy of Proof of Address (PoA) – for document based enrolment
- Copy of Date of Birth (DoB) ; in case of Verified Date of Birth only
- Copy of Proof of Relationship (PoR) in case of Head of Family (HoF) based enrolment
- Consent – for each enrolment

b. Ensure clarity and quality of submitted document copies.
c. Ensure correct documents are collected against PoI, PoA, DoB & PoR
d. Keep documents during enrolment in tray and do not fold them
e. Upon completion of enrolment, immediately collate the set of documents and staple it at left hand corner. Ensure documents for a resident are tagged together along with enrolment form on top. Ensure all documents in one set belong to one resident.
f. Store documents in proper box and avoid folding and excessive stacking
g. Protect documents from direct sun light, inflammable material, dust and water. It is recommended to use plastic covers to store set of documents to protect against environmental hazard.
h. Avoid writing on documents, this may create confusion for operators in later phases of the process
i. Avoid tying up documents using rope or packing tapes directly, this will permanently damage documents, if tying up is unavoidable use PET Straps with edge protectors
j. File documents in order of enrolment
k. Handle enrolment documents with care and protect from damage and theft.
l. Make sure to hand over the documents to your Supervisor/ other assigned authority at the end of the day

Maintaining Scanned Documents (when scanning process is introduced)

a. The Operator will scan Originals of each of the documents below depending on the type of enrolment:

- Enrolment Form – For each Enrolment
- PoI, PoA – For document based enrolments
- DoB document – For Verified Date of Birth
- PoR – For Head of Family Based Enrolments
- Acknowledgement cum Consent – For each Enrolment after Operator and Resident's signature

b. In instances where Original documents are not available, copies attested / certified by a public notary / gazetted officer will be accepted.
c. The documents are scanned in a sequence and all document scans are standard size (A4).
d. Make sure that the desired portions (the data entered during Aadhaar enrolment) of the document are visible clearly in the scan and the document pages do not overlap.
e. Each scanned page must be legible and without any marks due to dust and scratches. Remove the previous scan and re- scan a document where required.
f. Once all document pages are scanned, the Operator can see and check the total no. of pages scanned and confirm that all pages are scanned.
g. Return all the original documents and Enrolment Form to the resident. Also handover the acknowledgement cum Consent to the Resident.

How does the Operator perform Correction in Resident's Data?

Correction Process

a. For correction in any of the above data of a resident, the Operator must use Correction menu on software client. Resident data can be corrected within 96 hours of the resident's enrolment and in the presence of the resident.
b. The EA must restrict all corrections in a Residents data to only one time.
c. The following requests for changes are included in the scope of the Correction Process:

- All demographic fields i.e., Name, Address, Gender, Date of Birth / Age*
- Information sharing consent
- Relationship to resident
- Mobile
- Email Address
- NPR Receipt Number
- Relationship Details(Relation type, Name and EID/UID)
- Introducer Name and UID

d. If originally the resident was enrolled as a child below 5 years of age it is invalid to correct the resident age to above 5 years because for above 5 we require biometric data as well which would not have been captured during enrolment.

e. The previous Enrolment ID of the resident needs to be entered for correction of resident's old data. Check resident's acknowledgement letter for taking Enrolment number, date and time of enrolment for correction.
f. PoI, PoA and Parent/Guardian's acknowledgement letter will also be required at the time of correction process depending on the type of correction.
g. A change in Name would require either a verified Enrolment Form and PoI document or an Introducer's Name and UID. A change in Address would require either a verified Enrolment Form and PoA document or an Introducer's Name and UID. A change in verified DoB would require a verified Enrolment Form and DoB certificate. If the correction is in data for a child below 5 years of age, then parent details of relationship type, relative name and EID/UID of parent/guardian is also mandatory.
h. Only the fields that need a correction are entered in the Correction menu of the software. Fields that are good in original enrolment are not to be retyped during Correction. i. The resident's photo is also captured during correction process.
j. The correction in data will be reviewed with the resident and any one of the biometrics of the resident (provided in drop down menu on client) will also be taken to confirm that the resident is OK with corrections.
k. In case the resident is child below 5 years, the biometric of the parent/guardian whose details are entered in the relationship fields, will be taken. The Operator will sign off the enrolment and Supervisor, Introducer sign off will be required in biometric exceptions and Introducer based verification respectively.
l. An acknowledgement and consent of correction will be printed at the end of correction process along with the Resident's photo. The acknowledgement of correction will be signed by Operator and handed over to Resident. The consent will be signed by the resident and filed by the Operator along with the other documents of the resident.

Supervisor

Who is a Supervisor and what are his/her qualifications?

A Supervisor is employed by an Enrolment Agency to operate and manage enrolment centres. It is mandatory to have one Supervisor at each Enrolment Centre. To qualify for this role, the person should satisfy the following criteria:

a. The person should be of age 18 years and above.
b. The person shall be 10+2 pass and should preferably be a graduate
c. The person should have a good understanding and experience of using a computer
d. The person should preferably have prior experience of working in Aadhaar Enrolment program

Before starting work as a Supervisor:

a. The Supervisor should have been enrolled for Aadhaar and his/her Aadhaar number should have been generated.
b. The Supervisor should have undergone training on the process of UID Enrolment and various equipment and devices used during Aadhaar enrolment.
c. The Supervisor should have obtained certificate from a testing and certification agency appointed by UIDAI.
d. For certification, Supervisor needs to register with UIDAI appointed certification agency for taking the test at a suitable time and test centre location.
e. Supervisor must ensure that the Name and EID/UID provided during registration for test is same as that entered during Aadhaar Enrolment.
f. The Supervisor should have been activated in accordance with UIDAI guidelines prior to commencing enrolments. The Enrolment Agency is required to have a unique ID for each, to activate them.

What are the responsibilities of an EA's Supervisor?

At the Enrolment Centre, Supervisor's role is to plan and deploy logistics and other requirements at the enrolment centre, setup the enrolment stations at the enrolment centre and supervise the operations at the centre. When performing his/her role as a Supervisor at an Aadhaar Enrolment Centre, the Supervisor ensures the following:

1. **Site Readiness**

a. Enrolment Centre Setup Checklist is provided by UIDAI to facilitate the Enrolment Agency in setting up enrolment stations and centres. Supervisor must use the Enrolment Centre setup checklist to ensure that all requirements are met for the centre that he/she is responsible for. He/she must fill and sign the checklist at the beginning of each enrolment centre and/or once every week (whichever is earlier). This checklist needs to be maintained for later review/audit at every enrolment centre by Registrar/UIDAI and their nominated performance monitors/agency.
b. Supervisor is responsible for setting up of the laptop/desktop with Aadhaar client installed and tested, attached with all devices and printer (or scanners when mandated) and ensure all equipment are in working condition to start Aadhaar Enrolments.
c. Ensure that the latest Aadhaar Enrolment client software is installed.
d. Ensure that the enrolment centre premises are neat and clean, hygienic, well maintained and safe from electric/fire hazards.
e. Ensure that basic enrolment centre information as given below is displayed (in local language/English):

- Name of Registrar and Contact Number
- Name of EA & Contact Number
- Working hours
- Holidays

- Help Line Number;1800 180 1947
- Do not leave the centre without your acknowledgement receipt.
- Name, Code, and contact number of EA Supervisor at enrolment centres

f. Supervisor will also make sure that the Aadhaar IEC material provided by the Registrar is properly displayed at the centre, as per UIDAI guidelines.
g. Ensure that the behaviour of staff at the enrolment centre is courteous towards the residents. Take charge where operator is not able to handle dissatisfied resident and prevent unpleasant situations.
h. Where uniforms are provided, make sure that staff wears uniform at enrolment centre so that if residents need help they can easily identify employees by their attire.
i. Do not undertake enrolment operations at locations without valid agreement with the Registrars.

2. **On Boarding self and others**

a. Supervisor must first get on boarded himself/herself by providing their own biometrics in the Aadhaar client software. On-board (Enrolled) User means user's biometric details verification at UIDAI is successfully completed and stored in local database at the enrolment station.
b. Supervisor must make sure that all the Operators and Introducers for the enrolment centre are also on-boarded at the stations for local authentication.

3. **Managing Centre Operations**

a. Supervisor administers the enrolment process at his/her enrolment centre. He/she ensures adherence to the UIDAI enrolment processes and guidelines at the centre and good quality of data captured.
b. Supervisor handles issues and concerns of operators and residents and manages escalations at the centre level.
c. Supervisor also acts as an operator, when required, in exigencies.
d. Supervisor is required to sign off every enrolment on Aadhaar client, where resident has a biometric exception.
e. The EA Supervisor must ensure that every Operator is aware of and has a print copy of the critical points to be reviewed at the station during Resident's review of enrolment data.
f. Supervisor must make sure that the Operator diligently reviews the data captured with resident for every enrolment and making corrections when pointed out by the resident.
g. It is important that the Supervisor ensures that acknowledgement and consent are being printed after every enrolment and the printer and printing stationary is available for the same.
h. Supervisor can hold End of Day meeting at the centre for sharing learning of the day and issues faced.
i. Supervisor must take stock of the centre at the end of the day and make arrangements for replacement of faulty devices, hardware and other logistics for smooth enrolments the next day.
j. Check devices periodically for scratches, out of focus images, only partial images getting captured. In case any such problem is noticed, it should be reported to the Manager/HQ and a change of equipment should be requested.
k. Ensure all devices and computers are shut down. Check power is off to avoid accidents. Ensure security arrangements for devices and other equipments.

l. Specific End of Day Reports are available on the client, for selected time period, to facilitate EA Operations. Supervisor can make use of these reports in managing day to day operations at the centre.
m. Supervisor must ensure that staff at the centre observes the highest standards of ethics during the execution of Aadhaar Enrolments programme.
n. Supervisor is also responsible for maintaining the confidentiality and security of the documents, data collected during Aadhaar enrolments.

4. **Backup, Sync and Export**

a. Supervisor ensures twice a day data backup of all enrolment data to external hard disk as per UIDAI guidelines. Record date and station number where backup done to ensure that all stations are backed up and none is missed.
b. Supervisor also ensures that enrolment stations are synched at least once in every 10 days.
c. Supervisor manages timely data export of enrolment data for uploading to UIDAI server.
d. Supervisor can maintain a register for data exported. Record date, station number and packets exported at each station for reconciliation purpose.
e. Supervisor must correlate consent for enrolments to number of packets exported. Both numbers should match.

5. **End of Day Review**

a. Supervisor must Review all enrolments of the day, End of Day (EoD), to ensure that data entered in the Aadhaar client is correct for each resident. Supervisor may also deploy a fellow operator on-boarded on the machine for end of day review. However, the operator who did the enrolment cannot review his/her own packets.
b. In case any error/logical mismatch is found in the data entered, inform the resident to come to the enrolment centre within correction time frame. Supervisor must sign off by giving his/her fingerprint after End of Day Review.
c. Once correction is done to the resident's data, the Supervisor will again manually Approve/ Reject the Resident's packet put on Hold earlier for correction, with appropriate reason if rejected.

6. **Document Management**

a. Supervisor also ensures safe handling and storage of enrolment documents as per UIDAI guidelines and transfer of the same to Registrar/UIDAI DMS agency (as per the instructions of the Registrar).
b. Ensure one file/tray per station is maintained for documents storage
c. Ensure dockets (set of documents for a resident) in the order of enrolment and create a manifest of all documents.
d. Create document batch with manifest in soft copy and hardcopy along with exception list (if any).
e. Store documents/boxes indoor in a safe and secure place protected from fire, water and sabotage.
f. Keep the documents/boxes in a lockable place with proper ventilation till transfer/pickup
g. Once critical volume of dockets is reached/at the designated frequency by the registrar,

makes sure all the EID dockets are moved securely to offices designated by the Registrar.
h. Transport documents from enrolment centre to designated office only in properly sealed boxes tagged with manifest and packing list
i. Handle enrolment documents with care and protect it from damage and theft.
j. Avoid de-stapling, re-stapling or folding or excessive stacking of documents, it is recommended to store documents in boxes.

7. **Performance Monitoring**

a. The Supervisor cooperates with the UIDAI/Registrar's monitors in performing monitoring and audit functions at the enrolment centre and answers their questions to the best of his/her knowledge. Supervisor details are recorded during performance monitoring and Supervisor also signs on the performance monitoring sheet along with the monitor.
b. Supervisor ensures audit feedback, if any, is incorporated in process for continuous improvement of enrolment operations and data quality.

Updation in Aadhaar

What fields can I update through Self Service Update Portal (SSUP)?

Name, gender, DoB, address and mobile number can be updated using SSUP.

Can I request to Update fields by sending request through Post?

Yes, you can submit request for Name, gender, DoB, address and mobile number update through Post mode.

Can I get the information in my Aadhaar letter corrected using Update process?

Yes, Update modes can be used for corrections as well as changes in information.

I have lost my mobile number/ do not possess the number that I enrolled with in Aadhaar. How should I submit my Update request?

In case you have lost/do not possess anymore, the mobile, that you have declared at the time of enrolment, you will have to either visit the nearest Update Centre to personally update the information or send your Update request through Post.

What are the valid documents for submission of Update request through Portal /Post?

Depending on the field to be updated, attach self attested supporting documents as per the Valid Documents List.

Name Correction/Update – Requires PoI listed in "Supported Proof of Identity(PoI) Documents Containing Name and Photo for Name Corrections/Update"
Date of Birth Correction – Requires DoB listed in "Supported Proof of Date of Birth (DoB) Documents"
Address Corrections/Change – Requires PoA listed in "Supported Proof of Address (PoA) Documents Containing Name and Address"

Is it mandatory to provide Mobile number details when submitting Update Request through Post/online portal?

Yes, it is mandatory to provide mobile number as it may be used for Verification by calling the Applicant. Status of application will be intimated to the resident by sending an sms on this mobile number. Applications without mobile number for update through post/online will be rejected.

Is affidavit accepted as a PoI?

No. it is not accepted. Refer list of valid documents for acceptable PoI/PoA.

Is a certificate from local MP/MLA/local body official accepted as a proof document?

Certificate of Address having photo issued by MP or MLA or Gazetted Officer or Tehsildar on letterhead is acceptable as a Proof of Address.

Is it mandatory to provide C/o Details in Address?

No, it is not mandatory to provide c/o details with address. C/o details in address is used for letter delivery purposes and is a part of address.

Do I need to submit PoA even if I have to correct my C/O details only?

Yes, you are required to submit supporting PoA even if you want to update/correct only C/o details. You also have to fill the complete address when updating/correcting your C/o details or any other part of the address. The address in PoA must match the address in PoA document submitted.

My PoA does not mention C/o Details.

It is ok if C/o details are not mentioned in your PoA document. Use any valid PoA document that has the same address as the address mentioned in your Update Request.

My PoA does not mention C/o Details.

It is ok if C/o details are not mentioned in your PoA document. Use any valid PoA document that has the same address as the address mentioned in your Update Request.

Is there any standard form that I should use for sending update request through post?

Yes, use the standard "Aadhaar Data Update/Correction Form" published on UIDAI website. "AADHAAR DATA UPDATE/CORRECTION FORM FOR REQUEST THROUGH POST" is clearly mentioned on top of the form.

When sending request through Post, do I need to fill all fields even if I have to submit request for changes in only one particular field?

Yes, you must fill the complete form irrespective of the field/s for update/correction. Providing mobile number is mandatory for Update/Change in any of the fields. However, providing email ID is optional. Moreover, the fields required to be updated should be clearly indicated in the form.

Do I need to fill the form in English as well as Local language?

Yes, both in case of SSUP as well as Update requests through Post, fill the form in English as well as Local Language. Use the same local language that was used at the time of your enrolment in Aadhaar and appears in your Aadhaar Letter.

When I type Pin Code, it says Invalid Pin Code?

The Pin Code you are providing does not exist in our Pin Code master. Please ensure that you are typing a correct and valid Pin code. If you are still unable to find the Pin Code, you may use the option of sending your update request through Post.
Contact Center can also create a request for Pin Code addition/correction in the Pin Code portal. The user name and password have already been shared with the Contact Center.

I am unable to locate required Village/Town/City/Post office (PO)/District/State in the given Pin Code?

The required data does not exist in our Pin Code master. Please ensure that you are typing the correct Pin code. If you are still unable to find the required data, you may use the option of sending your update request through Post. Pin Code Update takes time, therefore, please try after 4weeks.
Contact Center can also create a request for Pin Code addition/correction in the Pin Code portal. The user name and password have already been shared with the Contact Center.

When I type in the English language field, local language data is not correctly transliterated. How should I correct it?

If the local language transliteration is not correct, go to the local language field on right hand side and retype in English. You may tweak the spelling a little to get the right phonetics and thus correct the local language spelling. Press tab key. If more than one option in local language appears on the local language field for the word, select the one that is correct. The instructions for transliteration are provided on the page where data entry is done. In case you are still finding issues in transliteration, you may send the request through Post.

Do I have to submit attested copies of documents? Who should attest my document copies?

Self attestation of the supporting documents is allowed. Resident's name must be clearly mentioned below the signatures when self attesting the documents. In case a child is below five years, parent/guardian can fill and sign in the form and document copies. In all other cases, the resident must sign in the form and document copies themselves.

Where should I send my request through Post?

Send the Form along with the supporting documents to UIDAI. Mark the envelope as **"Aadhaar Update/Correction"** on top. Seal the envelope properly. Depending on the local language in your Aadhaar data, send your request to one of the following UIDAI office addresses:

Does submission of request guarantee Updation of information?

Submission of information for update does not guarantee update of Aadhaar data. The information submitted is subject to verification and validation. Furnishing of incorrect information/suppression of information would lead to rejection of application and would attract penal provisions under the prevailing laws.

How will I be informed of the Update request status?

Aadhaar letter with updates will be delivered at the given address only in case of Update/Correction in Name, Address, Date of Birth and Gender. For Update of Mobile number/Email ID, the notification will be sent on the given mobile number/email ID.

You can also track your request on Update portal using your Update Request Number (14 digit URN).

How many Update requests can I submit?

Maximum permissible update request for each resident till March 2014 is limited to four. Repeated efforts to change/update the same field will attract investigations for establishing authenticity of the request.

I want to get demographic data in my Aadhaar updated/corrected. What should I do?

You can update Name, gender, DoB, address and mobile number either by submitting request Online or by sending your request through post. Visit www.uidai.gov.in and follow the link for "Update you Aadhaar Data".

NPR FAQs 101

Census of India : Frequently Asked Questions

FAQ for Public

FAQ for Public

A. What is Census? How is it useful?

Top

The Indian Census is the most credible source of information on Demography (Population characteristics), Economic Activity, Literacy & Education, Housing & Household Amenities, Urbanization, Fertility and Mortality, Scheduled Castes and Scheduled Tribes, Language, Religion, Migration, Disability and many other socio-cultural and demographic data since 1872. Census 2011 will be the 15th National Census of the country. This is the only source of primary data at village, town and ward level. It provides valuable information for planning and formulation of polices for Central & State Governments and is widely used by National & International agencies, scholars, business people, industrialists, and many more. The delimitation/reservation of Constituencies - Parliamentary/Assembly/Panchayats and other Local Bodies is also done on the basis of the demographic data thrown up by the Census. Census is the

basis for reviewing the country's progress in the past decade, monitoring the on-going schemes of the Government and most importantly, plan for the future. That is why the slogan of Census 2011 is "Our Census, Our Future".

B. What is the National Population Register? What is its use? Top

The NPR would be a Register of usual residents of the country. The NPR will be a comprehensive identity database that would help in better targeting of the benefits and services under the Government schemes/programmes, improve planning and help strengthen security of the country. This is being done for the first time in the country.

C. How will both these exercises be conducted? Top

The Census is a statutory exercise conducted under the provisions of the Census Act 1948 and Rules made there under. The NPR is being created under the provisions of the Citizenship Act and Rules.

Census Process:

The Census process involves visiting each and every household and gathering particulars by asking questions and filling up Census Forms. The information collected about individuals is kept absolutely confidential. In fact this information is not accessible even to Courts of law. After the field work is over the forms are transported to data processing centres located at 15 cities across the country. The data processing will be done using sophisticated software called Intelligent Character Recognition Software (ICR). This technology was pioneered by India in Census 2001 has become the benchmark for Censuses all around the globe. This involves the scanning of the Census Forms at high speed and extracting the data automatically using computer software. This revolutionary technology has enabled the processing of the voluminous data in a very short time and saving a huge amount of manual labour and cost.

NPR Process:

Details such as Name, Date of Birth, Sex, Present Address, Permanent Address, Names of Father, Mother and Spouse etc will be gathered by visiting each and every household. All usual residents will be eligible to be included irrespective of their Nationality. Each and every household will be given an Acknowledgement Slip at the time of enumeration. The data will then be entered into computers in the local language of the State as well as in English. Once this database has been created, biometrics such as photograph, 10 fingerprints and probably Iris information will be added for all persons aged 15 years and above. This will be done by arranging camps at every village and at the ward level in every town. Each household will be required to bring the Acknowledgement Slip to such camps. Those who miss these camps will be given the opportunity to present themselves at permanent NPR Centres to be set up at the Tehsil/Town level. In the next step, data will be printed out and displayed at prominent places within the village and ward for the public to see. Objections will be sought and registered at this stage. Each of these objections will then be enquired into by the local Revenue Department Officer and a proper disposal given in writing. Persons aggrieved by such order have a right of appeal to the Tehsildar and then to the District Collector. Once this process is over, the lists will be placed in the Gram Sabha in villages and the Ward Committee in towns. Claims and Objections will be received at this stage also and dealt with in the same manner described above. The Gram Sabha/Ward Committee has to give its clearance or objection within a fixed period of time after which it will be deemed that the lists have been cleared. The lists thus authenticated will then be sent to the Unique Identity Authority of India (UIDAI) for de-duplication and issue of UID

Numbers. All duplicates will be eliminated at this stage based on comparison of biometrics. Unique ID numbers will also be generated for every person. The cleaned database along with the UID Number will then be sent back to the Office of the Registrar General and Census Commissioner, India (ORG&CCI) and would form the National Population Register. As the UID system works on the basis of biometric de-duplication, in the case of persons of age 15 years and above (for whom biometrics is available), the UID Number will be available for each individual. For those below the age of 15 years (for whom biometrics is not available), the UID Number will be linked to the parent or guardian.

D. Will an Identity Card be given? Top

The National Population Register would have the data of every person enumerated during the Census operations irrespective of age. It would also have the biometric data and UID Number of every person of age 15 years and above. National Identity Cards will be given in a phased manner to all usual residents by the Office of the Registrar General and Census Commissioner, India. The issue of Cards will be done in Coastal Villages to start with. After this the coastal Towns will be covered and so on till the entire country is covered.

E. Who will collect the Information? Top

Government servants duly appointed as Enumerators will visit each and every house and collect the information required. They will carry an Identity Card as well as an Appointment Letter. In case of need you may ask them to show these documents. The local Tahsildar can also be contacted in this regard.

F. What information will be collected? Top

Two Forms will be canvassed in each household. The first relates to the Houselisting and Housing Census. In this, 35 questions relating to Building material, Use of Houses, Drinking water, Availability and type of latrines, Electricity, possession of assets etc. will be canvassed.
The second form relates to the National Population Register. In this the following will be canvassed:

* Name of the Person
* Gender
* Date of Birth
* Place of Birth
* Marital Status
* Name of Father
* Name of Mother
* Name of Spouse
* Present Address
* Duration of stay at Present Address
* Permanent Address
* Occupation
* Nationality as Declared
* Educational Qualification
* Relationship to Head of family

G. Will my Information be disclosed to anybody? Top

All information collected under the Census is confidential and will not be shared with

any agency - Government or private. Certain information collected under the NPR will be published in the local areas for public scrutiny and invitation of objections. This is in the nature of the electoral roll or the telephone directory. After the NPR has been finalised, the database will be used only within the Government.

H. How will I know that Census is being conducted? Top

The dates on which Census is being conducted in various States/Union Territories is given below:

Date of commencement	States /UTs
1st April	New Delhi (NDMC area), West Bengal, Assam, A & N Islands, Goa, Meghalaya
7th April	Kerala, Lakshadweep, Orissa, Himachal Pradesh, Sikkim
15th April	Karnataka, Arunachal, Chandigarh
21st April	Gujarat, Dadra & Nagar Haveli, Daman & Diu
26th April	Tripura, Andhra Pradesh
1st May	Haryana, Chhattisgarh, Delhi, Punjab, Uttaranchal, Maharashtra
7th May	Madhya Pradesh
15th May	J & K, Manipur, Mizoram, Rajasthan, Uttar Pradesh
1st June	Tamil Nadu, Puducherry, Himachal Pradesh (non synchronous), Nagaland
Not finalised	Bihar, Jharkhand

Advertisements will be published in local Newspapers and in the radio/electronic media. Apart from this, the Census enumerators will be visiting your house in person. They will be affixing small Census stickers on the doorway of houses in which Census has been completed. These will indicate that they have commenced operations in your area.

I. Whom do I contact in case my house is not covered? Top

The local Tehsildar/Ward Officer of your area is the designated officer. In case of need you can also contact the Collector/DC/DM of your District or the Commissioner of your Town. You can also intimate us over e mail or contact us over the toll free number given in this website.

J. How do I ensure that the information given by me is being correctly entered? Top

The NPR form has to be signed by you. In case you require, ask the Enumerator to read it out to you and then affix your signature/thumb impression. In any case do ascertain that the details are correctly entered.

K. Do I need to show any documents to the enumerator? Top

The enumerator will take down all particulars as given by you. You are not required to show any proof. However, be cautioned that it is expected that you will provide

correct and authentic information. You are also signing to this effect. The provision of false information can invite penalties under the Census and Citizenship Acts.

L. What is the Link between NPR and Unique ID Authority of India (UIDAI)? Top

The data collected in the NPR will be subjected to de-duplication by the UIDAI. After de-duplication, the UIDAI will issue a UID Number. This UID Number will be part of the NPR and the NPR Cards will bear this UID Number. The maintenance of the NPR database and updating subsequently will be done by the Office of Registrar General and Census Commissioner, India.

M. How people working abroad will be registered in National Population Register? Top

This is a Register of Usual Residents. If a person is staying at a particular place in India for 6 months in the past one-year or intends to stay there(in India) for at least 6 months in the future, they will be covered. If you are not a usual resident you will not be included in the NPR.

N. Can I send my census/NPR information electronically ? Top

No, however you can download blank schedules from census website from schedule section and keep the information ready. This may help Enumerators when he/she will come to your place for collecting/recording the information in the actual schedules especially designed for the census/NPR.

This website belongs to the office of The Registrar General & Census Commissioner, India, New Delhi, Ministry of Home Affairs, Government of India. Use of this site indicates that you accept the Terms of Use

106

भारतीय विशिष्ट पहचान प्राधिकरण
भारत सरकार

आधार

ENROLMENT FORM (आवेदन पत्र)

Please use CAPITAL letters (कृपया स्पष्ट अक्षरों में भरें) AADHAAR enrolment under : .....

Date (दिनांक) : .. / .. / ....

Part A - Primary Details/ (अ) प्राथमिक जानकारी

Name :
(नाम) : .....

☐ Mother माता ☐ Father पिता ☐ Husband पति Guardian's Name अभिभावक का नाम .....

(Name of Mother/Father/Guardian is must for children below 5 years of age)
(5 वर्ष से कम उम्र के बच्चों के लिये माता / पिता / अभिभावक का नाम अनिवार्य है)

Date of Birth : If not known, Age
जन्म तिथि : ..... / ..... / .... यदि नहीं पता, उम्र

Gender : ☐ Male पुरुष ☐ Female स्त्री ☐ Transgender अन्य
लिंग :

Residential address/आवास का

C/o .....

House No. and name/घर का नम्बर और नाम .....

Street No. and name /गली/सड़क नम्बर और नाम .....

Landmark /मुख्य पहचान .....

Village/City/गाम / शहर

District/जिला ..... Ranchi .....

State/राज्य : ..... Jharkhand Pin Code / पिन कोड : ☐☐☐☐☐☐

Part B - Additional Information/ (ब) अन्य जानकारी

Phone No./Mobile No. (Optional)/फोन नम्बर / मोबाईल नम्बर (ऐच्छिक) .....

E-mail (Optional/ ई-मेल (ऐच्छिक) .....

Part C - Financial Information/ (स) वित्तीय जानकारी .....

☐ I want to link my existing bank A/c to Aadhaar and I have No. this issue.
मैं चाहता / चाहती हूँ कि मेरे वर्तमान बैंक खाते को आधार के साथ जोड़ दिया जाए एवं इससे मुझे कोई आपत्ति नहीं है।

Bank name and Branch / बैंक का नाम व शाखा : .....

A/c No./ (शाखा संख्या) : .....

107

भारतीय विशिष्ट पहचान प्राधिकरण
योजना आयोग, भारत सरकार

आधार

ENROLMENT FORM (आवेदन पत्र)

Please use CAPITAL letters (कृपया स्पष्ट अक्षरों में भरें)
Date (दिनांक): _ _ / _ _ / _ _ _ _

AADHAAR/enrolment number: .....
आधार/आवेदन संख्या: .....

Part A – Primary Details / (क) प्राथमिक जानकारी

Name:
(नाम): _____

☐ Mother माता ☐ Father पिता ☐ Husband पति ☐ Guardian's Name अभिभावक का नाम _____

(Name of Mother/Father/Guardian is must for children below 5 years of age)
(5 वर्ष से कम उम्र के बच्चों के लिये माता/पिता/अभिभावक का नाम अनिवार्य है)

Date of Birth:
जन्म तिथि: _ _ / _ _ / _ _ _ _

If not known, Age: _ _ _
यदि नहीं पता, उम्र: _ _ _

Gender: लिंग: ☐ Male पुरुष ☐ Female स्त्री ☐ Transgender अन्य

Residential address: आवासीय पता:
c/o: _____
House No. and name: घर का नम्बर और नाम: _____
_____
Street No. and name: मोहल्ला/गली नम्बर और नाम: _____
_____
Landmark: मुख्य पहचान: _____
Village / City: ग्राम/शहर: _____
District: जिला: _____

State: राज्य: _____ Pin code: पिन कोड: ☐☐☐☐☐☐

Part B - Additional Information / (ख) (अन्य जानकारी)

Phone No. / Mobile No. (optional): फोन नम्बर / मोबाइल नम्बर (इच्छानुसार): _ _ _ _ _ _ _ _ _ _
Email (optional): ईमेल (इच्छानुसार): _____

Part C - Financial Information / (ग) वित्तीय जानकारी

☐ I want to link my existing bank A/c to Aadhaar and I have no objection on this issue.
मैं चाहता/चाहती हूँ कि मेरे वर्तमान बैंक खाते को आधार के साथ जोड़ दिया जाए एवं इसमें मुझे कोई आपत्ति नहीं है।

Bank name and Branch (बैंक का नाम व शाखा) _____

A/c No. (खाता संख्या) _____

भारतीय विशिष्ट पहचान प्राधिकरण
भारत सरकार

108

AADHAAR ENROLMENT / CORRECTION FORM

AADHAAR

Aadhaar Enrolment is free and voluntary. Correction within 96 hours of enrolment is also free. No charges are applicable for Form and Aadhaar Enrolment. In case of Correction provide your EID, Name and only that field which needs Correction.

In case of Correction provide your EID No here: | | | | | | | | | | | | | | dd | mm | yyyy | hh: mm: ss |

Please follow the instructions overleaf while filling up the form. Use capital letters only.

1	Pre-Enrolment ID :	2	NPR Receipt/TIN Number :
3	Full Name:		
4	Gender: Male ( ) Female ( ) Transgender ( )	5	Age: Yrs OR Date of Birth: DD | MM | YYYY Declared ☐ Verified ☐
6	Address: C/o ( ) D/o ( ) S/o ( ) W/o ( ) H/o ( ) NAME		
	House No/ Bldg./Apt.		Street/Road/Lane
	Landmark		Area/locality/sector
	Village/Town/City		Post Office
	District	Sub-District	State
	E Mail	Mobile No | | | | | | | | | |	PIN CODE | | | | | |
7	Details of : Father ( ) Mother ( ) Guardian ( ) Husband ( ) Wife ( ) *For children below 5 years Father/Mother/Guardian's details are mandatory. Adults can opt to not specify this information, if they cannot/do not want to disclose.*		
	Name		
	EID/ Aadhaar No.: | | | | | | | | | | | | | dd | mm | yyyy | hh: mm: ss |		
8	I have no objection to the UIDAI sharing information provided by me to the UIDAI with agencies engaged in delivery of welfare services.		YES ( ) NO ( )
9	Select One of the Below (OPTIONAL) (This data cannot be Corrected after Enrolment) ☐ I want the UIDAI to facilitate opening of a new Bank/Post Office Account linked to my Aadhaar Number and have no objection to sharing my information for this purpose ☐ I have no objection to linking my present bank account provided here to my Aadhaar number State Bank Name/Branch IFSC Code Account No.		

Verification Type : Document Based ( ) Introducer Based ( ) Head of Family ( )

Select only one of the above. Select Introducer or Head of Family only if you do not possess any documentary proof of identity and/or address. Introducer and Head of Family details are not required in case of Document based Verification.

10	For Document Based (Write Names of the documents produced. Refer back side of this form for list of valid documents)	
a. POI		b. POA
c. DOB (Mandatory in case of Verified Date of Birth)		d. POR
11	For Introducer Based – Introducer's Aadhaar No. | | | | | | | | | | | |	For HoF Based - Details of : Father ( ) Mother ( ) Guardian ( ) Husband ( ) Wife ( ) HoF's EId/Aadhaar No.: | | | | | | | | | | | | | | | dd | mm | yyyy | hh: mm: ss |

I hereby confirm the identity and address of _____ as being true, correct and accurate.

Introducer/HoF's Name: Signature of Introducer/HOF

Consent

I confirm that information (including biometrics) provided by me to the UIDAI and the information contained herein is my own and is true, correct and accurate.

Applicant's signature/Thumbprint

Verifier's Stamp and Signature:

(Verifier must put his/her Name, if stamp is not available)

To be filled by the Enrolment Agency only : Date & time of Enrolment: _____

Instructions to follow while filling up the enrolment form

Field 2 NPR NUMBER	Resident may bring his/her National Population Register Survey slip (if available) and fill up the column.
Field 3 NAME	Write full name without salutations/titles. Please bring the original* Proof of Identity (POI) document. (See list A below). Variation in Resident's Name in contrast to PoI is permissible as long as the change is minor spelling only, without altering the Name in PoI document. For Example: If Resident's PoI reads "Preeti", then "Priti" can be recorded if Resident wants so.
Field 5 DOB / AGE	Fill in Date of Birth in DDMMYYYY format. If exact Date of Birth is not known, approximate age in Years may be filled in the space provided. Please bring the original Proof of Date of Birth (DoB), if available.(See list D below). Declared checkbox may be selected if Resident does not have a valid proof of Date of Birth document. Verified checkbox is selected where Resident has provided documents as proof of Date of birth.
Field 6 ADDRESS	Write complete address. Please bring the original Proof of Address (POA) document. (See list B below). Please note that the Aadhaar letter will be delivered at the given address only. • To include Parent / Guardian / Spouse name as part of the address, select the appropriate box and enter the name of the person. • Minor Corrections / Enhancements are permissible to make the address complete without altering the base address as mentioned in the POA document.
Field 7 RELATIONSHIP	• In case of children below 5 years, it is mandatory to provide father/mother/guardian details with their Aadhaar or EID number. • If the resident is not holding a Proof of Identity & using the Head of the Family identity for enrolment, it is mandatory to provide Head of the family's details with his/her Aadhaar or EID number. Please refer illustration below for filling EID. Please bring the original Proof of Relationship (POR) document. (See list C below). • For other cases, it is optional for the resident to fill up the relationship details.
Field 8 CONSENT	Resident may specifically express willingness / unwillingness by selecting the relevant box.
Field 9 BANK ACCOUNT	Resident may choose to open a new Aadhaar enabled bank / POSB account or can link existing bank account to Aadhaar number. Relevant details as requested may be provided. This is an optional field.
Field 10 DOCUMENTS	Write the name of Documents for PoI and PoA. In case proof of Date of Birth is available, then write the name of Date of Birth document. If the resident is not holding a Proof of Identity & using the Head of Family based enrolment, then write the name of Proof of Relationship document. For Valid list of documents, please refer list of Documents below.
Field 11 INTRODUCER/HoF	Resident who does not have POI and POA may get enrolled through an Introducer/ Head of Family. Pl contact nearest enrolment centre or your Registrar, for further details.

List A. POI documents

1. Passport
2. PAN Card
3. Ration/ PDS Photo Card
4. Voter ID
5. Driving License
6. Government Photo ID Cards/ service photo identity card issued by PSU
7. NREGS Job Card
8. Photo ID issued by Recognized Educational Institution
9. Arms License
10. Photo Bank ATM Card
11. Photo Credit Card
12. Pensioner Photo Card
13. Freedom Fighter Photo Card
14. Kissan Photo Passbook
15. CGHS / ECHS Photo Card
16. Address Card having Name and Photo issued by Department of Posts
17. Certificate of Identify having photo issued by Gazetted Officer or Tehsildar on letterhead
18. Disability ID Card/handicapped medical certificate issued by the respective State/UT Governments/Administrations

List B. POA documents

1. Passport
2. Bank Statement/ Passbook
3. Post Office Account Statement/Passbook
4. Ration Card
5. Voter ID
6. Driving License
7. Government Photo ID cards/ service photo identity card issued by PSU
8. Electricity Bill (not older than 3 months)
9. Water bill (not older than 3 months)
10. Telephone Landline Bill (not older than 3 months)
11. Property Tax Receipt (not older than 3 months)
12. Credit Card Statement (not older than 3 months)
13. Insurance Policy
14. Signed Letter having Photo from Bank on letterhead
15. Signed Letter having Photo issued by registered Company on letterhead
16. Signed Letter having Photo issued by Recognized Educational Instruction on letterhead
17. NREGS Job Card
18. Arms License
19. Pensioner Card
20. Freedom Fighter Card
21. Kissan Passbook
22. CGHS / ECHS Card
23. Certificate of Address having photo issued by MP or MLA or Gazetted Officer or Tehsildar on letterhead
24. Certificate of Address issued by Village Panchayat head or its equivalent authority (for rural areas)
25. Income Tax Assessment Order
26. Vehicle Registration Certificate
27. Registered Sale / Lease / Rent Agreement
28. Address Card having Photo issued by Department of Posts
29. Caste and Domicile Certificate having Photo issued by State Govt.
30. Disability ID Card/handicapped medical certificate issued by the respective State/UT Governments/Administrations
31. Gas Connection Bill (not older than 3 months)
32. Passport of Spouse
33. Passport of Parents(in case of Minor)

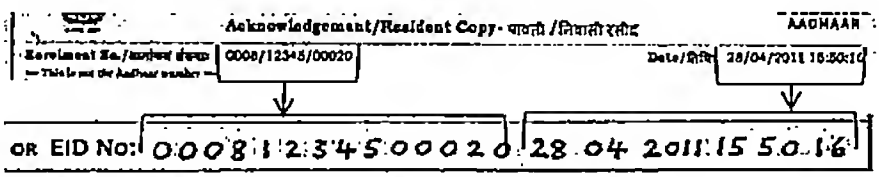
List C. POR documents

1. PDS Card
2. MNREGA Job Card
3. CGHS/State Government/ECHS/ESIC Medical card
4. Pension Card
5. Army Canteen Card
6. Passport
7. Birth Certificate issued by Registrar of Birth, Municipal Corporation and other notified local government bodies like Taluk, Tehsil etc.
8. Any other Central/State government issued family entitlement document

List D. DOB documents

1. Birth Certificate
2. SSLC Book/Certificate
3. Passport
4. Certificate of Date of Birth issued by Group A Gazetted Officer on Letterhead

Illustration for filling up EID No.



*In instances where original documents are not available, copies attested / certified by a public notary / gazetted officer will be accepted.

सत्यमेव जयते

110

NATIONAL POPULATION REGISTER

It is mandatory for all usual residents (citizens as well as non-citizens) to register in the National Population Register (NPR) under the Citizenship Act, 1955.

NPR camps will be held in every locality for collection of biometric data of all residents who are of age 5 years and above. **All usual residents are required to attend the NPR camp, even if their biometrics have been captured under Aadhaar.** Such persons already enrolled with Aadhaar are required to bring their Aadhaar letter/enrollment slip to the NPR camps.

For persons not so far enrolled under UIDAI, Aadhaar will be generated through NPR.

Date, time and venue of the NPR camp will be intimated by local authorities. **Please fill all applicable columns of the KYR+ form supplied to you and bring it to the camp.**

It is proposed to issue Resident Identity (smart) Cards bearing the Aadhaar number under the NPR.

Registration in NPR is a right as well as a duty of every resident.

सत्यमेव जयते

BIOMETRIC ENROLMENT FOR NATIONAL POPULATION REGISTER

1.11

During the Houselisting Operations (HLO) of Census 2011 held in May-June 2010, the enumerator had visited e household and collected identity details of all usually residing household members for the database of the Natio Population Register (NPR). An Acknowledgement Slip had been given in each household, to be furnished at the time collection of biometrics (photograph, fingerprints & iris scan).

It is hereby informed that the **NPR biometric collection camp for your Enumeration Block** is to take place at the following date, place and time:

LOCATION:

DATE: **TIME:**

The biometrics of all household members, who were recorded as **usual residents** of the household at the time of HLO/N in 2010, and who are now **above 5 years of age,** are to be collected. Please make it convenient to visit the camp and get biometric enrolment done. **Enrolment with NPR is mandatory as per Citizenship Act 1955 and Citizenship Ru 2003.**

In case any household member is not in a position to travel to the camp due to **disability or infirmity,** kindly inform enumerator accordingly. Their enrolment will be arranged at the residence later.

Please bring your NPR Acknowledgement Slip. However, in case you have misplaced the Slip, you can find your name a serial number in the list of residents available at the camp itself.

In case you have **shifted recently** and were not covered in the NPR earlier at this address, kindly ensure that the enumera fills up a **fresh NPR form** for you. In such cases the biometrics will be collected during the second round to be held a f weeks later.

Please fill all applicable columns of the KYR+ format given below for every household member being enrolled a bring this form with you. Please also bring the original Ration Card, Voter Card, DL, PAN Card, Passport, whichever applicable, for verification of the Nos while feeding into the database.

At the camp, please verify that your particulars as fed in the computer database are **complete &correct.** Please exerc your option for Banking Consent & Information Sharing.

PLEASE NOTE THAT VISITING THE NPR CAMP IS MANDATORY EVEN IF YOU HAVE ALREADY BE ENROLLED FOR AADHAR/UID. In this case, please bring your Aadhar Letter/ pre- enrolment slip with you. You n not need to give Biometrics again subject to certain conditions.

Director of Citizen Registrati
Director of Census Operations, D

No._____ Household No_____

OW YOUR RESIDENT PLUS (KYR+) PARTICULARS: Please fill ALL applicable columns

tion Card No (Common for all household members) :

o.	Name of person in full	Voter ID Card No.	Driving Licence No.	PAN No.	Passport No

e, Mobile No, and signature of the Enumerator

Name and signature of the Respond

National Population Register Household Schedule

SIDE-A

Start Here

Location Particulars

State/UT | District | Tehsil/Taluk/P.S./Dev. Block/Circle/Mandal | Town/Village | Ward Code No. (only for Town)

To be copied from Houselisting Schedule: Houselisting Block Number | Household Number (from Column 9)

ENGLISH

Serial number	Q.1 Name of the person in full and resident status 1(a) Write name of the person in full (start with head of household) 1(b) Write resident status code in box Usual Resident (Actual)..... 1 Usual Resident (Interloper) .. 2 Others..... 3	Q.2 Name of the person as should appear in the National Population Register (maximum of 30 boxes, abbreviate if required)	Q.3 Relationship to head (record the relationship in full)	Q.4 Sex Male.... 1 Female.2	Q.5 Date of birth as per English calendar Day Month Year Write in the box Actual as A or Declared as D	Q.6 Marital status Never married .. 1 Currently married .. 2 Widowed.. 3 Separated..4 Divorced... 5	Q.7 Educational qualification	Q.8 Occupation/ Activity Describe the actual work	Q.9 Name(s) of father, mother and spouse in full If father, mother and spouse are not enumerated in this household or not alive write Father's name against 'F', Mother's name against 'M', Spouse's name against 'S' OR if they are enumerated in this household, write serial number of the father, mother and spouse in the boxes as recorded in column 1

Use only arabic numbers as indicated here

0 1 2 3 4 5 6 7 8 9

Form Number

National Population Register Household Schedule

SIDE-B

Serial number	Q.1 Name of the person Copy from Q. 1 (a) of side A in same order	Q.10 Place of birth If within India, write the present name of the Village/Town, District and State. If outside India, write the present name of the Country and put '–' against Village/Town and District.	Q.11 * Nationality as declared Indian – 1 Others write name of Country	Q.12 Present address of usual residence If the person resides or intends to stay for more than 6 months at this address (Write complete address including the (i) Building Number and Name, House Number, (ii) Street name, (iii) Locality/Post Office, (iv) Village/Town, (v) District, State)	Q.13 Duration of stay at present address (in completed years)	Q.14 Permanent residential address If same as Q.12 write 'Same' otherwise (Write complete address including the (i) Building Number and Name, House Number, (ii) Street name, (iii) Locality/Post Office, (iv) Village/Town, (v) District, State)

Providing any false information would attract penalties under the Citizenship Rules, 2003.

Use only arabic numbers as indicated here

0 1 2 3 4 5 6 7 8 9

Q.11 * NOTE
Nationality recorded in Q. 11 is as declared by the respondent. This does not confer any right to Indian Citizenship.

Name of the Respondent

Phone / Mobile of the Respondent

Serial Number

I declare that all the information provided above is true to the best of my knowledge and belief.

Signature/Thumb Impression (for male left thumb and for female right thumb) of Respondent with Date

Signature of the Enumerator with Date

Sex of Enumerator
Male
Female

Signature of the Supervisor with Date

Continued to another Sheet
Write 'C' if continued to another sheet

Write last three digits of the form number of the continued sheet

MEMORANDUM OF UNDERSTANDING
BETWEEN THE UNIQUE IDENTIFICATION AUTHORITY OF INDIA
AND
THE REGSITRAR GENERAL OF INDIA
FOR THE IMPLEMENTATION OF THE UID PROJECT

This Memorandum of Understanding (MoU) has been executed on the 16th March, 2011 between the Unique Identification Authority of India (hereinafter referred to as "UIDAI") and the Registrar General of India (hereinafter referred to as "The RGI").

Preamble

Whereas, the Government of India has set up Unique Identification Authority of India (UIDAI) with the mandate to issue Unique Identification Numbers (called "Aadhaar numbers") to all residents of India (UID project).

Whereas, the RGI is creating the National Population Register (hereinafter referred to as "The NPR") under the Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003 read with the Citizenship Act, 1955.

Whereas, in order to achieve convergence in the implementation of the UID project and the NPR exercise, the RGI is entering into this MoU with the UIDAI.

Whereas, this MoU shall come into effect from the date of execution of this MoU.

Definitions

Unless the Context requires otherwise;

Registrar means any entity authorised or recognised by the UIDAI for the purpose of enrolling individuals for UID numbers. Registrars include Departments or Agencies of the Central Government/ State Government/Union Territory, who, in normal course of implementation of some of their programs, activities or operations interact with residents and are authorized by the Central Governments/State Governments/Union Territories to enrol residents into the UID System.

Sub-Registrars are agencies of the RGI for undertaking enrolment.

Enrolling Agencies are entities hired by the Registrars/Sub-Registrars to perform enrolment functions.

UID Project and the scope of the MoU

1. The UIDAI has the mandate from the Government of India to issue unique identification numbers (UID numbers) to residents of India based on demographic and biometric data of the individual. UIDAI will partner with Government and other agencies leveraging their existing infrastructure in order to implement the UID project. These Agencies will be called the Registrars of UIDAI.

2. Several Registrars are embarking on capturing the biometrics and are ready to enrol residents into the UID system for better targeting and improving their service delivery. UIDAI has created necessary infrastructure to issue UID numbers through Multiple Registrars.

3. UIDAI shall set standards and processes for enrolment to be uniformly followed by all Registrars and Enrolling Agencies. The UIDAI will issue UID numbers after checking that the resident applying for UID does not already have a record and number in the UID database. In addition, the UIDAI will provide online Authentication service.

4. This MoU between the UIDAI and the RGI, as a Registrar, sets out below, the general and broad-based intentions of both Parties for collaboration and as an umbrella understanding for facilitation of subsequent agreements and documents relevant for the implementation of the UID project.

5. The UIDAI shall prescribe standards, procedures and processes for enrolment and authentication of residents which will be adhered to by the RGI/Sub-Registrars of RGI and enrolling agencies appointed by the Sub-Registrars.

6. In the interest of clarity and to reduce ambiguity, the UIDAI may execute additional agreements and documents to capture details about implementation of UID Project with RGI as Registrar.

7. UIDAI shall-
    a. Develop and prescribe standards for recording data fields, data verification and biometric fields.
    b. Prescribe a process for enrolment of residents; this will include among other things the process for collection of biometric data.
    c. Prescribe the standards and criteria to be fulfilled by an agency to be appointed as a Registrar.
    d. Provide/prescribe the software that will be used for the enrolment of people into the UID database in order to issue the UID numbers.
    e. De-duplicate the database of the residents on the basis of the Demographic and Biometric data and issue UID numbers to only those whose uniqueness of identity has been established and after ensuring that the person has not enrolled in the UID database before.
    f. Issue a letter communicating the UID number directly to the person who has been allotted UID number after de-duplication. UIDAI will also communicate the UID number electronically with the RGI in UIDAI prescribed format.
    g. Authenticate the identity of a person with a UID number as per the protocols prescribed by the UIDAI.

h. Prescribe protocols for record keeping and maintenance of the information collected for the issuance of a UID number.
i. Prescribe protocols for transmission of the data collected for de-duplication.
j. Prescribe protocols to ensure the confidentiality, privacy and security of data.
k. Prescribe limits for fees that could be charged for issuing a UID number.
l. Prescribe protocols for spreading and communicating the message, content and intent of the UID project. Since the UID logo and brand name are properties of the UIDAI, the UIDAI will prescribe the manner and limits of the use of UIDAI logo, brand name, brand design and other communication and awareness materials.
m. Prescribe other protocols, processes and standards that the UIDAI may deem necessary for the implementation of the UID project.
n. Call for information and records, conduct inspections and enquiries and audit of the operations pertaining to the UID project.
o. Conduct periodic audit of the enrolment process and to this end shall have the power to visit and inspect offices of the Sub-Registrar and Enrolling Agencies. Such audits are necessary to ensure the integrity of the enrolment process and to ensure uniformity across the country.
p. Prescribe mechanisms for resolution of grievances that the residents may have during enrolment and authentication.

8. The RGI shall-
   a. Co-operate and collaborate with the UIDAI in conducting proof of concept (PoC) studies and pilots to test the working of the technology and process of enrolment into the UID database.
   b. Be the Registrar for the implementation of the UID project (including PoC and pilots) and shall do all that is necessary and required in order to effectively complete the PoCs and pilots.
   c. Put in place an institutional mechanism to effectively oversee and monitor the implementation of the UID project in general and monitor specifically enrolling agents.
   d. Cooperate and collaborate with and provide all assistance and support to the Deputy Director Generals (DDGs) concerned of the UIDAI and other staff members/consultants/advisors of the UIDAI to effectively implement the UID project.
   e. Provide logistic and liaison support to the staff and representatives of UIDAI when they visit the Enrolling agencies enrolling under the UID project on behalf of RGI.
   f. Work with the UIDAI to resolve difficulties faced on the ground in the implementation of the UID project.
   g. Follow the process set out by the UIDAI for resolution of difficulties and conflict regarding matters concerning the UID project.

9. The following is an indicative list of the obligations of the Registrar. Notwithstanding anything contained in this clause, this list can be expanded or elaborated as required to ensure integrity and uniformity of enrolment into the UID database. In order to implement the UID project, the RGI shall-
    a. Either do the enrolment directly or through Enrolment Agencies who shall be identified and appointed by RGI or his duly appointed agents (UIDAI may recommend certain criteria to be fulfilled to be an Enrolling Agency). The Enrolling Agencies will be working on behalf of RGI and their duly appointed agents and will be accountable to them. However, they should follow all the standards, protocols, processes laid down by the UIDAI to implement the UID project. RGI must ensure compliance by the Enrolling Agencies of the standards, protocols, processes laid down by the UIDAI on a continuous basis.
    b. Follow the standards for data fields, data verification and biometric fields prescribed by the UIDAI.
    c. Follow the process for enrolment of residents; this will include among other things the process for collection of biometric data prescribed by the UIDAI.
    d. Use the software developed by the UIDAI for the enrolment of people into the UID database for the issuance of the UID number.
    e. Use only those devices and IT systems whose specifications have been approved by the UIDAI.
    f. Follow the protocols prescribed by the UIDAI for record keeping and maintenance.
    g. Follow the process and systems prescribed by the UIDAI for transmission of the data collected for de-duplication.
    h. Follow the confidentiality, privacy and security protocols prescribed by the UIDAI.
    i. The Registrars can collect any data in addition to what is prescribed by the UIDAI for the purpose of rendering any service based on UID number.
    j. Follow protocols prescribed by the UIDAI for spreading and communicating the message, content and intent of the UID project, Since the UID logo and brand name are properties of the UIDAI, the UIDAI will prescribe the manner and limits of the use of UIDAI logo, brand name, brand design and other communication and awareness materials.
    k. Follow protocols, processes and standards prescribed by the UIDAI for the implementation of the UID project.
    l. Allow the UIDAI to conduct periodic audit of the enrolment process and to visit and inspect the offices and records of the Sub-Registrar and Enrolment Agencies and any other place the UIDAI or its empowered agency may deem necessary for their purpose.
    m. Submit information and records, allow inspections and inquiries and audit of the operations pertaining to the UID project.

n. Submit periodic reports of enrolment to the UIDAI in the form and manner prescribed by the UIDAI.
o. Provide logistic and liaison support to the staff and agents of UIDAI when they visit the offices of the RGI.
p. Provide information related to the UID project to the UID from time to time as requested by the UIDAI.
q. Work with the UIDAI to resolve difficulties faced on the ground in the implementation of the UID project.
r. Follow the process set out by the UIDAI for resolution of difficulties and conflict regarding matters concerning the UID project.

Miscellaneous

10. At the time of collecting data for the purpose of the UIDAI, RGI may collect data from the resident that is required for the purpose of creating NPR.

11. In situations where the processes and standards for enrolment set by the UIDAI are not followed or are violated (wilfully or otherwise) by the Sub-Registrar and/or an Enrolling agency, the UIDAI shall make reasonable attempts to discuss and attempt to resolve difficulties with RGI. Pursuant to which if the recommendations of the UIDAI are not implemented and the matter settled to the satisfaction of both the parties, the UIDAI shall have the option to de-register or demand replacement of the enrolling agency as the case maybe.

12. Any provision of this MoU may be amended or waived if, and only if, such amendment or waiver is evidenced by a written instrument signed by duly authorised representatives of the Parties, or, in the case of a waiver, by the Party against whom the waiver is to be effective.

IN WITNESS WHEREOF, the undersigned have executed this MoU, in duplicate, as of the date set forth above.

On behalf of UIDAI	On behalf of RGI
(Anil Khachi)	(K.S. Sawhney)
Deputy Director General	Joint Secretary & Joint Registrar General of India

119

MEMORANDUM
OF
UNDERSTANDING

UNIQUE IDENTIFICATION AUTHORITY OF INDIA

And

GOVERNMENT OF NCT, DELHI

MEMORANDUM OF UNDERSTANDING
BETWEEN THE UNIQUE IDENTIFICATION AUTHORITY OF INDIA
AND
THE GOVERNMENT OF NCT OF DELHI FOR THE IMPLEMENTATION OF THE UID PROJECT.

This Memorandum of Understanding (MoU) has been executed on the 28th June, 2010 between the Unique Identification Authority of India, (hereinafter referred to as" UIDAI") and the Government of NCT of Delhi (hereinafter referred to as "The Govt. of NCT of Delhi").

PREAMBLE

Whereas, Government of India has set up UIDAI with the mandate to issue Unique Identification Numbers (UID) to all residents of India (UID Project).

Whereas, the Govt. of NCT of Delhi would like to enhance efficiency in delivery of governmental benefits and services through accurate identification of beneficiaries and to have uniform standards and processes for verification and identification of beneficiaries;

Whereas, in order to implement the UID Project in NCT of Delhi, the Govt. of NCT of Delhi is entering into this MoU with the UIDAI;

Whereas, the Govt. of NCT of Delhi has set up State UID Implementation Committee vide order no. 21(6)/2009/ Co-ord/Plg/949-70 dated 23rd June, 2010 to oversee the implementation of the UID Project in the NCT of Delhi. The said Committee consists of Chief Secretary as Chairman, Divisional Commissioner as Member Secretary, Principal Secretary, Finance, Chief Electoral Officer, Commissioner Transport, Secretary Social Welfare, Commissioner, Food & Civil Supplies, Secretary Information & Technology, Secretary, Labour, All Deputy Commissioners, Representative of Commissioner Census GOI, Representative of UIDAI, Director Planning and MD, Mission Convergence as members;

Whereas, this MoU shall come into effect from 28th June, 2010.

DEFINITIONS

Unless the context requires otherwise,

Registrars are departments or agencies of the Govt. of NCT of Delhi, which in normal course of implementation of some of their programs or activities interact with the residents, and are authorized by the Govt. of NCT of Delhi to enroll residents into the UID system. Examples of such Registrars are Rural Development Department (for NREGS) or Civil Supplies and Consumer Affairs Department (for TPDS).

Enrolling Agencies are entities hired by the Govt. of NCT of Delhi or Registrars to perform enrolment functions on behalf of the Registrar(s).

UID Project and the Scope of the MoU

1. The UIDAI has the mandate from the Government of India to issue Unique Identification numbers (UID) to residents of India based on demographic and biometric data of the individual. UIDAI will partner with governments and other agencies leveraging their existing infrastructure in order to implement the UID Project. These agencies will be called the Registrars of UIDAI.

2. UIDAI will set standards and processes for enrolment to be uniformly followed by all Registrars and Enrolling Agencies. The UIDAI will issue UIDs after checking that the resident applying for UID does not already have a record and UID in the UID database. In addition, the UIDAI will provide online, real-time authentication service.

3. The UID Project will be implemented in a phased manner. The UIDAI will be conducting proof of concept studies and pilots to test the working of the technology and process of enrolment and would require the co-operation of the Govt. of NCT of Delhi and Registrars in this regard.

4. This MoU between the UIDAI and the Govt. of NCT of Delhi sets out below, the general and broad-based intention of both the parties for collaboration and as an umbrella understanding for facilitation of subsequent agreements and documents relevant for the implementation of the UID Project in the of NCT of Delhi.

5. The UIDAI shall prescribe standards, procedures and processes, which will be adhered to by the Registrars identified/appointed by the Govt. of NCT of Delhi.

6. In the interest of clarity and to reduce ambiguity, the UIDAI shall execute additional agreements and documents to capture details about implementation of UID Project with Registrars identified / appointed by the Govt. of NCT of Delhi.

7. UIDAI shall:
   a. Develop and prescribe standards for recording data fields, data verification and biometric fields.
   b. Prescribe a process for enrolment of residents; this will include among other things the process for collection of biometric data.
   c. Prescribe the standards and criteria to be fulfilled by an agency or department to be appointed as Registrar.

d. Provide / prescribe the software that will be used for the enrolment of people into the UID database in order to issue the UID.
e. De-duplicate the database of the residents on the basis of the demographic and biometric data and issue UIDs to only those whose uniqueness of identity has been established and after ensuring that the person has not enrolled in the UID database before.
f. Issue a letter communicating the UID directly to the person who has been allotted UID after de-duplication. UIDAI will also simultaneously communicate the UID electronically with the Registrar in UIDAI-prescribed format.
g. Authenticate the identity of a person with UID number as per the protocols prescribed by the UIDAI.
h. Prescribe protocols for record keeping and maintenance of the information collected for the issuance of a UID.
i. Prescribe Protocols for transmission of data collected for de-duplication.
j. Prescribe protocols to ensure the confidentiality, privacy and security of data.
k. Prescribe limits for fees that could be charged for issuing a UID.
l. Prescribe protocols for spreading and communicating the message, content and intent of the UID Project. Since the UID logo and brand name are properties of the UIDAI, the UIDAI will prescribe the manner and limits of the use of UIDAI logo, brand name, brand design and other communication and awareness materials.
m. Prescribe other protocols, processes and standards that the UIDAI may deem necessary for the implementation of the UID Projects.
n. Conduct periodic audit of the enrolment process and to this end shall have the right to visit and inspect offices of the Registrar and Enrolling Agencies. Such audits are necessary to ensure the integrity of the enrolment process and to ensure uniformity across the country.
o. Prescribe mechanisms for resolution of grievances that the residents may have during enrolment and authentication.

8. The Govt. of NCT of Delhi shall:

a. Co-operate and collaborate with the UIDAI in conducting proof of concept (PoC) studies and pilots to test the working of the technology and process of enrolment into the UID database.
b. Identify Registrars for the implementation of the UID Project (including PoC and pilots). Ensure that the Registrar shall do all that is necessary and required in order to effectively complete the PoCs and pilots.
c. Follow the criteria and process for appointment of Registrars and Enrolling Agencies prescribed by the UIDAI.
d. Put in place an institutional mechanism to effectively oversee and monitor the implementation of the UID Project in general and monitor specifically registrars and Enrolling Agencies appointed by the Registrar.
e. Provide required financial and other resources to the Registrars to carry out the enrolment processes as per the phasing decided by the Govt. of NCT of Delhi.
f. Cooperate and collaborate with, and provide all assistance and support to the Deputy Director Generals (DDG) concerned of the UIDAI and other staff member /consultants /advisors of the UIDAI to effectively implement the UID Project in NCT of Delhi.

g. Provide logistic and liaison support to the staff and representatives of the UIDAI when they visit the Registrar and Enrolling Agencies implementing the UID Project.
h. Work with the UIDAI to resolve difficulties faced on the ground in the implementation of the UID Project.
i. Follow the processes set out by the UIDAI for resolution of difficulties and conflicts regarding matter concerning the UID Project.

9. The following is an indicative list of the obligations of the Registrars. Notwithstanding anything contained in this clause, this list can be expanded or elaborated as required to ensure integrity and uniformity of enrolment into the UID database. In order to implement the UID Project, the Registrars shall:

a. Either do the enrolment directly or through Enrolment Agencies who shall be identified and appointed by the Registrars (UIDAI may recommend certain criteria to be fulfilled to be an Enrolling Agency). The Enrolment Agencies will be working on behalf of the Registrars and will be accountable to the Registrars. Therefore, they should follow all the standards, protocols, processes laid down by the UIDAI to implement the UID project. Registrars must ensure compliance by the Enrolling Agencies of the standards, protocols, processes laid down by the UIDAI on a continuous basis.
b. Follow the standards for data fields, data verification and biometric fields prescribed by the UIDAI.
c. Follow the processes prescribed by the UIDAI for enrolment of residents. This will include among other things the process for collection of biometric data.
d. Use the software developed by the UIDAI for the enrolment of people into the UID System.
e. Use only those devices and IT systems whose specifications have been approved by the UIDAI.
f. Follow the protocols prescribed by the UIDAI for record keeping and maintenance.
g. Follow the processes and systems prescribed by the UIDAI for transmission of data collected for de-duplication.
h. Follow the confidentiality, privacy and security protocols prescribed by the UIDAI.
i. The Registrars can collect any data in addition to what is prescribed by the UIDAI for the purpose of rendering any service based on UID number.
j. Have the option to charge a fee for the UID service but the fees charged from residents cannot be higher than the maximum amount prescribed by the UIDAI in this regard.
k. Follow protocols prescribed by the UIDAI for spreading and communicating the message, content and intent of the UID Project. Since the UID logo and brand name are properties of the UIDAI, the UIDAI will prescribe the manner and limits of the use of UIDAI logo, brand name, brand design and other communication and awareness materials.
l. Follow protocols, processes and standards prescribed by the UIDAI for implementation of the UID Project.
m. Allow the UIDAI to conduct periodic audit of the enrolment process and to visit and inspect the offices and records of the Registrar and Enrolment Agencies and any

other place the UIDAI or it's empowered agency may deem necessary for their purpose.

n. Submit periodic reports of enrolments to the UIDAI in the form and manner prescribed by the UIDAI.

o. Provide logistic and liaison support to the staff and agents of the UIDAI when they visit the Registrar and Enrolling Agencies implementing the UID Project in NCT of Delhi.

p. Provide information related to the UID Project to the UIDAI from time to time, as requested by the UIDAI.

q. Work with the UIDAI to resolve difficulties faced on the ground in the implementation of the UID Project.

r. Follow the process set out by the UIDAI for resolution of difficulties and conflict regarding matters concerning the UID Project.

s. Take any other measure for fulfilling the obligations effectively.

Miscellaneous

10. In situations where the processes and standards for enrolment set by the UIDAI are not followed or are violated (willfully or otherwise) by the Registrar and /or an Enrolling Agency, the UIDAI shall make reasonable attempts to discuss and attempt to resolve difficulties with the Govt. of NCT of Delhi. Pursuant to which if the recommendations of the UIDAI are not implemented and the matter settled to the satisfaction of both the parties, the UIDAI shall have the option to de-register the concerned Registrar and /or demand replacement of the concerned Enrolment Agency as the case may be.

11. Any provision of this MoU may be amended or waived if, and only if, such amendment or waiver is evidenced by a written instrument signed by duly authorized representatives of the Parties, or in the case of a waiver, by the party against whom the waiver is to be effective.

IN WITNESS WHEREOF, the undersigned have executed this MoU, in duplicate, as of the date set forth above.

On behalf of UIDAI	On behalf of Govt. of NCT of Delhi
(NIRMAL KUMAR SINHA)	**(D.M. Spolia)**
Deputy Director General	Pr. Secretary (Revenue)/ Divisional Commissioner
Unique Identification Authority of India	GNCT OF DELHI
Planning Commission	
GOVERNMENT OF INDIA	

125

MEMORANDUM OF UNDERSTANDING
BETWEEN THE UNIQUE IDENTIDICATION AUTHORITY OF INDIA
AND
THE GOVERNMENT OF TAMIL NADU
FOR THE IMPLEMENTATION OF THE UID PROJECT

This Memorandum of Understanding (MoU) has been executed on 10th day of August 2010 between the Unique Identification Authority of India (hereinafter referred to as "UIDAI") and the Government of TamilNadu (hereinafter referred to as "The State Government")

Preamble

Whereas, the Government of India has set up Unique Identification Authority of India (UIDAI) with the mandate to issue Unique Identification Numbers (UID numbers) to all residents of India (UID project).

Whereas, the State Government would like to enhance efficiency in delivery of government benefits and services through accurate identification of beneficiaries and to have uniform standards and processes for verification and identification of beneficiaries.

Whereas, in order to implement the UID project in the State of TamilNadu, the Government of TamilNadu is entering into this MoU with the UIDAI.

Whereas, the Government of TamilNadu has set up a State Level Advisory Board under the Chairmanship of the Chief Secretary to monitor and resolve issues related to the implementation of the Unique Identification Number Project. The Revenue Department of the State Government has been identified as the Nodal Department for coordinating all activities related to the UID Project on behalf of the State Government.

Principal Secretary /
Commissioner of Revenue
Administration, Chepauk,
Chennai - 600 005.

Whereas, this MoU shall come into effect from the date of execution of this MoU.

Definitions

Unless the Context requires otherwise;

Registrars are Departments or Agencies of the State Government/Union territory, who, in normal course of implementation of some of their programs or activities interact with the Residents and are authorized by the State Government/Union Territories to enroll residents into the UID System. Examples of such Registrars are Rural Development Department (for NREGS) or Civil Supplies and Consumer Affairs Department (for TPDS).

Enrolling Agencies are entities hired by the State Government/ Union territory or Registrars to perform enrolment functions on behalf of the Registrar(s).

UID Project and the scope of the MoU

1. The UIDAI has the mandate from the Government of India to issue unique identification numbers (UID numbers) to residents of India based on demographic and biometric date of the individual. UIDAI will partner with Government and other agencies leveraging their existing infrastructure in order to implement the UID project. These Agencies will be called the Registrars of UIDAI.
2. UIDAI will set standards and processes for enrolment to be uniformly followed by all Registrars and Enrolling Agencies. The UIDAI will issue UID numbers after checking that the resident applying for UID does not already have a record and number in the UID database. In addition, the UIDAI will provide online, real-time Authentication service.

Principal Secretary /
Commissioner of Revenue
Administration, Chepauk,
Chennai - 600 005.

3. The UID project will be implemented in a phased manner, the UIDAI will be conducting proof of concept studies (PoCs) and pilots to test the working of the technology and process of enrolment and would require the co-operation of the State Government/Union territory and Registrars in this regard.
4. This MoU between the UIDAI and the Government of TamilNadu sets out below, the general and broad-based intentions of both parties for collaboration and as an umbrella understanding for facilitation of subsequent agreements and documents relevant for the implementation of the UID project in the State of TamilNadu.
5. The UIDAI shall prescribe standards, procedures and processes which will be adhered to by the Registrars identified/ appointed by the State Government.
6. In the interest of clarity and to reduce ambiguity, the UIDAI shall execute additional agreements and documents to capture details about implementation of UID Project with Registrars identified/ appointed by the State Government.

7. UIDAI shall

   a. Develop and prescribe standards for recording data fields, data verification and biometric fields.
   b. Prescribe a process for enrolment of residents; this will include among other things the process for collection of biometric data.
   c. Prescribe the standards and criteria to be fulfilled by an agency to be appointed as a Registrar.
   d. Provide/prescribe the software that will be used for the enrolment of people into the UID database in order to issue the UID numbers.

Principal Secretary /
Commissioner of Revenue
Administration, Chepauk,
Chennai 600 005.

e. De-duplicate the database of the residents on the basis of the Demographic and Biometric data and issue UID numbers to only those whose uniqueness of identity has been established and after ensuring that the person has not enrolled in the UID database before.

f. Issue a letter communicating the UID number directly to the person who has been allotted UID number after de-duplication. UIDAI will also communicate the UID number electronically with Registrar in UIDAI prescribed format.

g. Authenticate the identity of a person with a UID number as per the protocols prescribed by the UIDAI.

h. Prescribe protocols for record keeping and maintenance of the information collected for the issuance of a UID number.

i. Prescribe protocols for transmission of the data collected for de-duplication.

j. Prescribe protocols to ensure the confidentiality, privacy and security of data.

k. Prescribe limits for fees that could be charged for issuing a UID number.

l. Prescribe protocols for spreading and communicating the message, content and intent of the UID project. Since the UID logo and brand name are properties of the UIDAI, the UIDAI will prescribe the manner and limits of the use of UIDAI logo, brand name, brand design and other communication and awareness materials.

m. Prescribe other protocols, processes and standards that the UIDAI may deem necessary for the implementation of the UID project.

n. Conduct periodic audit of the enrolment process and to this end shall have the power to visit and inspect offices of the Registrar and Enrolling Agencies. Such audits are necessary to ensure the integrity of the enrolment process and to ensure uniformity across the country.

o. Prescribe mechanisms for resolution of grievances that the residents may have during enrolment and authentication.

p. Evolve a suitable funding mechanism for enrolment of residents into the UID system.

8. The State Government shall

a. Co-operate and collaborate with the UIDAI in conducting proof of concept (PoC) studies and pilots to test the working of the technology and process of enrolment into the UID database.

b. Identify Registrars for the implementation of the UID project (including PoC and pilots). Ensure that the Registrar shall do all that is necessary and required in order to effectively complete the PoCs and pilots.

c. Follow the criteria and process for appointment of Registrars and enrolling agencies prescribed by the UIDAI.

d. Put in place and institutional mechanism to effectively oversee and monitor the implementation of the UID project in general and monitor specifically Registrars and enrolling agents appointed by the Registrar.

e. Provide required financial and other resources to the Registrars to carry out the enrolment processes as per the phasing decided by the State Government/ Union territory.

f. Cooperate and collaborate with and provide all assistance and support to the Deputy Director Generals (DDGs) concerned of

the UIDAI and other staff members/consultants/advisors of the UIDAI to effectively implement the UID project in the State of TamilNadu.

g. Provide logistic and liaison support to the staff and representatives of UIDAI when they visit the Registrar and Enrolling agencies implementing the UID project.

h. Work with the UIDAI to resolve difficulties faced on the ground in the implementation of the UID project.

i. Follow the process set out by the UIDAI for resolution of difficulties and conflict regarding matters concerning the UID project.

9. The following is an indicative list of the obligations of the Registrars. Notwithstanding anything contained in this clause, this list can be expanded or elaborated as required to ensure integrity and uniformity of enrolment into the UID database. In order to implement the UID project the Registrars shall.

a. Either do the enrolment directly or through Enrolment Agencies, who shall be identified and appointed by the Registrars (UIDAI may recommend certain criteria to be fulfilled to be an Enrolling Agency). The Enrolment Agencies will be working on behalf of the Registrars and will be accountable to the Registrars; therefore they should follow all the standards, protocols, processes laid down by the UIDAI to implement the UID project. Registrars must ensure compliance by the enrolling Agencies of the standards, protocols, processes laid down by the UIDAI on a continuous basis.

b. Follow the standards for data fields, data verification and biometric fields prescribed by the UIDAI.

Principal Secretary /
Commissioner of Revenue
Administration, Chepauk,
Chennai - 600 005.

c. Follow the process for enrolment of residents; this will include among other things the process for collection of biometric data prescribed by the UIDAI.

d. Use the software developed by the UIDAI for the enrolment of people into the UID database for the issuance of the UID number.

e. Use only those devices and IT systems whose specifications have been approved by the UIDAI.

f. Follow the protocols prescribed by the UIDAI for record keeping and maintenance.

g. Follow the process and systems prescribed by the UIDAI for transmission of the data collected for de-duplication.

h. Follow the confidentiality, privacy and security protocols prescribed by the UIDAI.

i. Have the option to charge a fee for the UID service but the fees charges from residents cannot be higher than the maximum amount prescribed by the UIDAI in this regard.

j. Follow protocols prescribed by the UIDAI for spreading and communicating the message, content and intent of the UID project, Since the UID logo and brand name are properties of the UIDAI, the UIDAI will prescribe the manner and limits of the use of UIDAI logo, brand name, brand design and other communication and awareness materials.

k. Follow protocols, processes and standards prescribed by the UIDAI for the implementation of the UID project.

l. Allow the UIDAI to conduct periodic audit of the enrolment process and to visit and inspect the offices and records of the Registrar and Enrolment Agencies and any other place the UIDAI or its empowered agency may deem necessary for their purpose.

Principal Secretary /
Commissioner of Revenue
Administration, Chepauk,
Chennai-600 005.

m. Submit periodic reports of enrolment to the UIDAI in the form and manner prescribed by the UIDAI.

n. Provide logistic and liaison support to the staff and agents of UIDAI when they visit the Registrar and Enrolling agencies implementing the UID project.

o. Provide information related to the UID project to the UID from time to time as requested by the UIDAI.

p. Work with the UIDAI to resolve difficulties faced on the ground in the implementation of the UID project.

q. Follow the process set out by the UIDAI for resolution of difficulties and conflict regarding matters concerning the UID project.

Miscellaneous

10. In situations where the processes and standards for enrolment set by the UIDAI are not followed or are violated (willfully or otherwise) by the Registrar and/or an Enrolling agency, the UIDAI shall make reasonable attempts to discuss and attempt to resolve difficulties with the State Government. Pursuant to which if the recommendations of the UIDAI are not implemented and the matter settled to the satisfaction of both the parties, the UIDAI shall have the option to de-register the concerned Registrar and / or demand replacement of a concerned Enrolment agency as the case maybe.

11. Any provision of this MoU may be amended or waived if, and only if, such amendment or waiver is evidenced by a written instrument signed by duly authorised representatives of the Parties, or, in the case of a waiver, by the Party against whom the waiver is to be effective.

IN WITNESS WHEREOF, the undersigned have executed this MoU, in duplicate, as of the date set forth above.

On behalf of UIDAI

Ashok Mahadeorao Dalwai
Deputy Director General,
Regional Office, Bengaluru,
Unique Identification Authority of India,
Planning Commission
Government of India

Dr. Ashok Dalwai, IAS
Deputy Director General
Unique Identification Authority of India
R.O. Bangalore

On behalf of State Government

Dr.N.Sundaradevan
Principal Secretary/ Commissioner,
Revenue Administration Department,
Government of TamilNadu

UID AND PUBLIC HEALTH

The Unique Identification (UID) project is a historic venture that seeks to provide a unique registration code to every Indian citizen. We surmise that the starting point would be to aggregate records from various population databases such as the census, the PDS system, voter identity systems, etc, while dealing with the challenge of duplication.

Existing data bases would probably still leave a large percentage of the population uncovered. Therefore every citizen must have a strong incentive or a "killer application" to go and get herself a UID, which one could think of as a demand side pull. The demand pull for this needs to be created *de novo* or fostered on existing platforms by the respective ministries. Helping various ministries visualise key applications that leverage existing government entitlement schemes such as the NREGA and PDS will (1) get their buy-in into the project (2) help them roll out mechanisms that generate the demand pull and (3) can inform a flexible and future-proof design for the UID database. It will also build excitement and *material support* from the ministries for the UID project even as it gets off the ground.

Health, and health related development schemes could offer a killer application for the UID. After years of neglect, public health in India is seeing a revolution both in terms of (1) greater commitment towards government financing of public and primary healthcare (2) pressure to meet the MDG goals (3) consequent creation of large supply platforms at national levels such as the NRHM, RSBY and complementary state level initiatives such as the Rajiv Arogyasri insurance scheme in Andhra Pradesh. In health there is a cumulative historic gap both in terms of demand and supply. The UID could further help catalyse a revolution in India's health outcomes.

What would be the public health associated payoff through the application of the UID?

Major challenges in public health today include (1) lack of detailed denominator (ie target population to be covered) focussed services delivery by the government's rural and urban healthcare systems at district and sub-district levels (2) poor tracking of health conditions by for example, the ICD-10 disease classification system and (3) lack of ability to roll out at scale, expansion of ambitious national health insurance schemes like the RSBY.

Thus for example, India's coverage of its annual birth cohort of 27 million children through childhood vaccinations has been stagnating at circa 55% for the most elementary bouquet of vaccines. Similarly antenatal check-up coverage of the roughly 27 million pregnant women is nationally about 52%, and only 47% of women deliver in institutions. While the first is a problem related to poor denominator tracking at the lowest level of the government's public health system by frontline health workers, the second additionally also poses a challenge of appropriately administering such demand side incentive schemes such as the JSY to increase institutional births.

Routine health information systems (including vital registration, cause of death identification, disease reporting) that capture and track the morbidity and mortality due to various disease

conditions are critical to improving public health outcomes including life expectancy. Currently infrequent national or state surveys are the major mode of capturing data on infectious disease conditions. However, chronic or lifestyle diseases are not captured in any meaningful way even through surveys. These pose new challenges for an already strained public health system. An integrated routine health system that can capture and track population level disease conditions by linking citizen ids with hospital or other medical facility records generated through facility visits can (1) inform the public health system of the prevalence of various routine disease conditions (2) help prepare the health system to respond to unforeseen epidemics. A partial example of (1) above can be seen under the Rajeev Arogyasri insurance scheme in Andhra Pradesh, but taking this to scale across the country will require coordination between the UID project, the Ministry of Health and the Ministry of Labour (see below).

The launch of the RSBY (Rashtriya Swasthya Bima Yojana) by the Ministry of Labour is a great example of a killer app waiting for a platform. Launched about fourteen months ago, it is intended to eventually provide in some form or other in partnership with states, the country's entire population with insurance coverage. Since launch only approximately 5.4 million individuals in some 370 districts of 18 states have been covered. RSBY does include the provision of a card and supports a putatively large but very simple field registration effort. Partnering with this scheme will (1) provide an additional and fresh, unlikely to be duplicated source of registrations for the UID and (2) more importantly, in conjunction with linkages to a routine health information system can improve public health in terms of efficiency and outcomes.

UID and NREGA

Background

Launched in 2006, the National Rural Employment Guarantee Scheme (NREGS) is an attempt to transform the rural economy through legally guaranteed employment for up to 100 days per household. The scheme, run jointly by the Centre and the states, has a total budget allocation of Rs. 39,100 crores, which is 8.1% of the total plan budget for the fiscal year 2008-2009. The NREGS has reached several milestones towards its goal, but suffers from the same challenges like most other public projects — corruption and diversion of funds. Incidents of guaranteed minimum wages being denied to workers have been reported from nearly every state where the program is currently functional[1].

When implemented and adopted efficiently, the Unique Identification (UID) project possesses the power to eliminate financial exclusion, enhance accessibility, and uplift living standards for the majority poor. This can be achieved when the UID is effectively associated with pro poor welfare projects like the NREGS. The Unique Identification Authority of India (UIDAI) aims to issue a unique identification number to all Indian residents that is (a) robust enough to eliminate duplicate and fake identities, and (b) can be verified and reliably authenticated in an easy, cost-effective way. The ability of UID to positively establish and authenticate the identity of every individual can overcome many of the challenges faced by targeted benefit programs.

UID Ready NREGS

To effectively leverage the UID program, the NREGS scheme will need to be modified to incorporate the UID number into beneficiary interactions. In order to accommodate UID authentication, NREGS will need to reengineer its business processes. The most basic requirement for change will be in the form of incorporating the UID method of authentication. Work sites will have to adhere to norms and procedures specified by the UIDAI for fingerprint capture and verification, and introduce a robust biometric authentication process at every point.

The key areas in the NREGS process that need to be addressed are summarized below:

- UID in Job Cards – The job cards will need to be updated with the UID numbers of all family members. This could be accomplished by issuing a new job card or by

[1] The GB Pant Social Science Institute at Allahabad University reported that officials and contractors in Orissa siphoned off 32 percent of the funds, depriving 90 days of wage employment to about 10 lakh poor families in the state.

collecting and incorporating the UID numbers into the beneficiary database without reissue of the job cards.

- **UID in Muster Rolls** – The muster rolls should contain a reference to the UID of the citizen who is earning wages. This should be incorporated at the time of allocation of the labor to the project (works).

- **UID in Bank account** – The UID should be incorporated with the bank / post office account information of a beneficiary to which the wages are being paid. A mechanism to encourage bank / post office to incorporate the UID into their systems is being pursued.

- **Transaction Authentication** - The transaction authentication against the UID database should be implemented at different citizen touch points starting with the job card. The ideal situation would be the recording of attendance on a handheld system using biometric authentication. UID will also endeavor to introduce a biometrics authentication for amount withdrawal from the account into which wages are paid.

The above change can be implemented in the NREGS program with minimal effort. There are also synergies with other government programs such as TPDS that can be explored that can further ease the implementation in areas such as handheld deployment.

UID Powered NREGS

Incorporation of UID into the NREGS program will assist in addressing some of the major challenges that impedes progress. The major areas that can be addressed and ways of addressing them are described in this section:

- Payment of Wages - Payment of wages remains one of the major challenges faced in NREGS. Wherever possible these payments are supposed to be automated through local bank branches or through post offices. In many areas the wages continue to be paid in the form of cash. The UID can fully replace the need to provide supporting documentation for the standard Know Your Customer (KYC) fields making opening a bank account significantly simpler. Arrangements of seamlessly opening a bank account in the name of one of the family members at the time of job card issue with embedded UID can also be explored.

- **Theft from beneficiaries** - One form of corruption in NREGS is 'theft from beneficiaries' where officials under-paid workers for the work they have done[2]. The responsibility of determining and authenticating the amount of work done lies in the hands of the official supervisors who are prone to siphoning off funds. The system of UID authentication when introduced at the site of work can ensure that there is a match between the hours of work claimed by the worker and the official supervising the site. The ability of UID to identify the presence of a specific individual also makes it much easier to centrally monitor delinquency among government servants who are authenticating the work and checking whether the allocated work was completed satisfactorily.

- **Theft from Taxpayers** - The study also threw light on another form of corruption which the researchers called 'theft from taxpayers' wherein the officials over-reported the amount of work done when they sent their reports up the hierarchy. This effort can be corroborated against the wages paid to beneficiaries establishing the execution of the project. Suspicious activity can be flagged and verified by an appropriate government official.

- **Ghost Beneficiaries** – Once each citizen in a job card needs to provide his UID before claiming employment, the potential for ghost or fictitious beneficiaries is eliminated. A further reinforcement of paying only to real citizens will happen by way of opening bank accounts with UIDs.

- **Beneficiary Misuse** - UID will ensure that misuse by claiming benefits under multiple job cards is avoided. The UID de-duplication process which will assure a positive identification of every resident in the country, can overcome the challenge of uniquely identifying every worker.

- **Beneficiary Management** – The UID system will provide an excellent platform for managing citizens who relocate or migrate from one place to another and want to seamlessly enjoy benefits of the program.

- **Social Audit** - The village level social audit committee can be selected after authentication with the UID database. The social audit reports filed by the village level committees can be authenticated by the biometrics of the committee members and the social audit coordinator.

---

[2] Paper on "Corruption Dynamics: The Golden Goose Effect" by Sandeep Sukhtankar and Paul Niehaus of Harvard University

- Transparency – The above benefits combined with the positive beneficiary identification will ensure accurate details of benefits can be published providing greater transparency at the individual beneficiary level.

UID Enrollment by NREGS

The NREGS program provides an extensive reach and extensive citizen interaction opportunity. The NREGS program can be used to enrol residents into the UID program with the state machinery acting as the registrars. A resident seeking to get a job card and not having a UID can be enrolled into the UID system at the point of job card preparation. Necessary arrangements and business model for providing the necessary technology can be put in place.

The enrolment into the UID program by NREGS will provide a convenient mode for procuring a UID to rural citizens and strengthen both programs.

With convenient IT enabled systems, households with changes in the family structure due to death, birth or marriage as also relocation will update changes to their job cards which can be reflected in the UID database.

Summary

There are significant synergies between the NREGS and the UID program allowing improved implementation of the NREGS program with a increased transparency. The UID program benefits by increased enrolment and an opportunity to capture changes to beneficiary data.

UID AND PDS System

Objectives of Public Distribution System (PDS)

India's Public Distribution System (PDS) with a network of 4.78 Lakh Fair Price Shops (FPS) is perhaps the largest retail system of its type in the world. Since 1951 public distribution of food grains has been retained as deliberate social policy by India with the objectives of:

(i) Providing food grains and other essential items to vulnerable sections of the society at reasonable (subsidized) prices
(ii) To put an indirect check on the open market prices of various items and
(iii) To attempt socialization in the matter of distribution of essential commodities

PDS is an important constituent of the strategy for poverty eradication and is intended to serve as a safety net for the poor whose number is more than 33 Crores and are nutritionally at risk. PDS is operated under the joint responsibility of the Central and the State Governments. The Central Government has taken the responsibility for procurement, storage, transportation and bulk allocation of food grains, etc.

The operational details of the PDS differ from state to state. Though the policy of setting up of FPSs owes its initiation to national food policy, its implementation remains the direct responsibility of the state governments. In order to operate the PDS effectively, the Central Government issues guidelines from time to time to the states regarding the operational details of the PDS. The operational responsibilities including allocation within the State, identification of families below poverty line, issue of ration cards, supervision and monitoring the functioning of FPSs rest with the State Governments. The Food and Civil Supplies Department of the State Government is mainly entrusted with the task of monitoring PDS in the state.

Food Subsidy

Food Subsidy is provided in the budget of the Department of Food and Public Distribution to meet the difference between the economic cost of food grains and their sales realization at Central Issue Prices for TPDS (Targeted PDS) and other welfare schemes. In addition, the Central Government also procures food grains for meeting the requirements of buffer stock. Hence, part of the food subsidy also goes towards meeting the carrying cost of buffer stock. The subsidy is provided to FCI under TPDS and other welfare schemes and for maintaining the buffer stock of food grains as measure of food security.

The quantum of food subsidy depends on the level of procurement of food grains and offtake under TPDS and other welfare schemes. The budgetary estimate for food subsidy during 2008-09 was about Rs. 37,000 Crores.

PDS System Today

The TPDS system today supports over 40 Crore Indians below the poverty line with monthly supply of subsidized food grains. The system also provides gainful employment for 4.78 Lakh Fair Price Shops Owners, their employees and hired labour who work at the FCI and state warehousing godowns.

PDS also has become a cornerstone of government development policy and is tied to implementation of most rural development programs. PDS is also a key driver of public sentiment and is an important and very visible metric of government performance.

One of the main problems with this system is the inefficiency in the targeting of beneficiaries and the resulting leakage of subsidies. Several opportunities to manipulate the system exist with widespread collusion across the supply chain. The Planning Commission had the following to say on the PDS system in its 2005 report.

"For every Rs 4 spent on the PDS, only Rs 1 reaches the poor"

"57% of the PDS food grain does not reach the intended people"

The Challenges

There are many systemic challenges that plague the PDS system today and the key ones are described below:

1. *PDS Leakages* - The TPDS currently suffers from a number of issues that make it difficult for it to meet its objective of ensuring that the allotted quota of specified food articles reaches the intended underprivileged/needy segments of society:
   - A large number of families living below the poverty line have not been enrolled and therefore do not have access to ration cards
   - A number of bogus ration cards which do not correspond to real families, exist in the BPL & AAY categories. Food drawn on the basis of these bogus cards is a significant leakage from the system, as it does not reach the intended beneficiaries. Additionally, these extra cards inflate the number of BPL and AAY cards in circulation and further reduce the amount of food available to every rightful beneficiary family.
   - A number of instances where benefits are being availed in the names of rightfully entitled families without their knowledge. This shadow ownership is possible due to inefficiencies in ration card issuance and distribution
   - Errors in categorization of families that lead to BPL families getting APL cards and vice versa.
   - A significant portion of benefits provided to the APL category under the TPDS, are not availed by the intended beneficiaries and are instead diverted out of the system.

   In summary, targeting is not serving its real purpose, as the beneficiaries do not get food grains in accordance with their entitlements.

2. *Scale and Quality of Issue* – The scale of issue and the quality of food grains delivered to the beneficiary is rarely in conformity with the policy. Many FPS are open only for a few days in a month and beneficiaries who do not visit the FPS on these days are denied their right. The FPS also use multiple excuses to both charge higher rates and deliver reduced quantity of food grains.

   There are also significant differences in the manner in which the Centre and States arrive at the number of BPL families. This mismatch usually means lower allotments for each family as states arrive at higher numbers of BPL families.As this problem may not go away even after reduction of duplicates, a standard way of doing this must be arrived at for each state to resolve this issue.

3. *System Transparency and Accountability* –The most serious flaw plaguing the system at present is the lack of transparency and accountability in its functioning.The system lacks transparency and accountability at all levels making monitoring the system extremely difficult.

4. *Grievance Redressal Mechanisms* – There are numerous entities like Vigilance Committee, Anti-Hoarding Cells constituted to ensure smooth functioning of the PDS system. Their impact is virtually non-existent on the ground and as a result, malpractices abound to the great discomfiture of the common man.

Apart from the challenges described, transportation of food grains and appointment of dealers of Fair Price Shops have also become difficult issues. Viability of the FPS is already a major concern and this would get amplified once PDS leakages are brought under control.

The Proposed Food Security Act

The President's Address contains the following announcement regarding food security:

"My Government proposes to enact a new law – the National Food Security Act – that will provide a statutory basis for a framework which assures food security for all. Every family below the poverty line in rural as well as urban areas will be entitled, by law, to 25 kilograms of rice or wheat per month at Rs.3 per kilogram. This legislation will also be used to bring about broader systemic reform in the public distribution system."

Creation of a framework that assures food security for all and a broader systemic reform are the two operational components of the act apart from the commitment to provide 25 kg of rice or wheat at Rs.3 per kg to the BPL population.

The numerical size of the target BPL population will be determined by the Centre and identification of the individual poor households who will be entitled to BPL benefits in each state will have to be done by each State.

As per the *draft act*, the Centre will offer to each State its BPL entitlement of grain at the economic cost, with a separate subsidy covering the differences between the economic cost and the issue price. The State should have the option to either take the grain at economic cost from the Centre or to manage its own procurement from within the State, or anywhere else in the country, including from imports if they are economical. The Centre will transfer the subsidy entitlement irrespective of whether the State Government takes grain from the Centre or makes its own arrangements to procure grain.

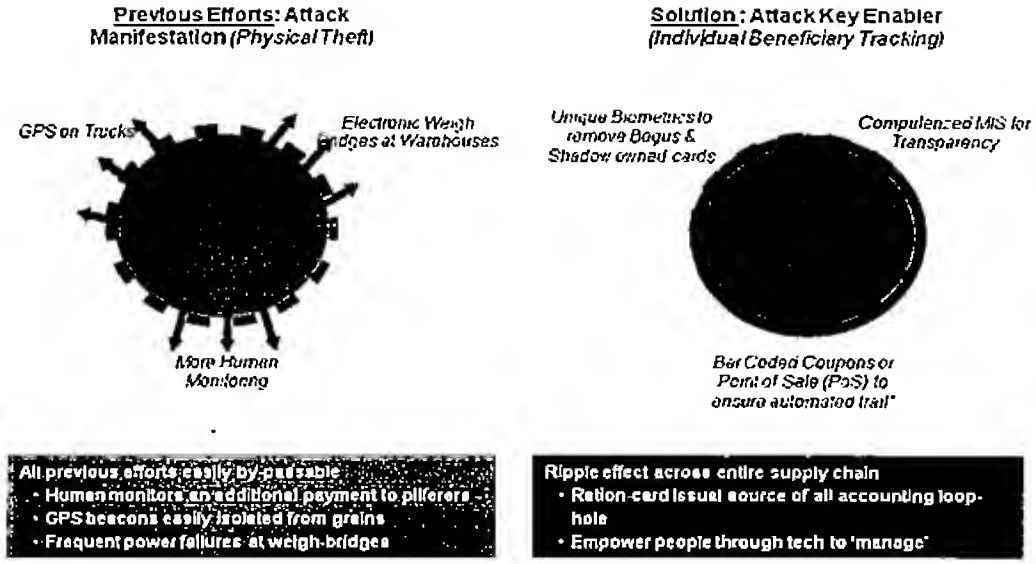
The State Government can provide the grain through PDS at the notified subsidized price or provide cash transfers of the subsidy amount to designated BPL households. It has also been recommended that when a cash transfer is made, it should be to a bank account in the name of the oldest women member of the household.

The systemic changes proposed provide the capability to implement far-reaching reforms. Systemic efficiency improving changes that can be explored include:

- **Roaming Ration Cards** providing an opportunity to short-term migrants to move their ration cards to their new area or work.
- **Direct Cash Transfer Program** where the subsidy will be transferred into the bank account of the beneficiary.
- **Choice of Fair Price Shops** should improve quality of service and this solution allows the incorporation of either limited or full choice of FPS.
- **Food Stamps** can be introduced allowing competition from existing food shops and increasing the reach of the TPDS network

Proposed IT based solution approach

A significant part of the challenges in the PDS system emanates from Bogus (ration cards belonging to fictitious families) and Shadow (genuine ration cards used by someone else) ration cards in the system. If the bogus cards can be substantially weeded out and a mechanism put in place to positively confirm and track the individual beneficiary offtake on a monthly basis, the problems relating to PDS leakages, Transparency and Transportation would get resolved, as leakage would become more difficult to hide.



Earlier attempts at addressing the challenges have focused on identifying the "Physical Theft" and used tools like additional Human monitoring, Global Positioning Systems (GPS) on trucks to track the movement of trucks and Electronic Weigh bridges. All these tools are easily by-passable and even if they work efficiently, cannot address the PDS leakages that predominantly stem from the bogus and shadow ration cards in the system.

A solution that improves the quality of the beneficiary database and can track Individual Beneficiary offtake coupled with a computerized MIS system can effectively improve the PDS system. By leveraging some of the large e-governance initiatives that are being rolled out, the solution can be implemented swiftly and cost effectively.

The Solution Components

The draft food security act implicitly requires a computerization of various elements of the PDS system. The key components of the proposed solution and how they can be implemented in a rapid and cost effective manner is briefly described in this section.

Creation of a Beneficiary Database

The state government should create a high quality beneficiary database, preferably commencing from a house-to-house survey. The State government can carry out the enrollment of identified family members by enrolling them into the UID (Unique ID) program.

After digitization of requisite information, enrollment of the individuals is carried out as per the UID requirements. The digitized database will contain ten finger biometrics and photographs[1] of all family members. This enrolled data would be sent to the UIDAI (Unique Identity Authority of India) for de-duplication and issual of a UID, which will be printed on the ration card for each member of the family.

Appropriate action can be taken against families that have a resident who has appeared in another ration card. Reasons for family members do are not enrolled has to be determined followed by appropriate action. The inclusion of all families in the beneficiary database is important for an effective elimination of Shadow and Bogus cards. A strategy to issue APL cards by linking it to other forms of benefits including LPG needs to be adopted to make the beneficiary database comprehensive.

To support enrollment into the UID database, the central government will mandate that the UID numbers of each family member should be recorded in the ration card and the database should be made available.

Individual Beneficiary Tracking

Eligible beneficiaries do not avail of their entire allotment due to various reasons that include unavailability of funds, usage of food grains grown by them and temporary migration, but most FPS owners tend to report a complete offtake. A mechanism is required to be put in place to accurately track the real offtake by beneficiaries.

[1] The number and type of biometrics will be finalized in due course

The ideal option is the deployment of a Point of Sale (PoS) system that is equipped with a fingerprint reader to positively identify a beneficiary before an issue is made. The PoS system can generate a receipt and automate the bookkeeping reducing the time required for a transaction. The data on eligible beneficiaries for the next month is transferred to the PoS each month with the offtake information for the previous month is collected.

Apart from ensuring accurate beneficiary offtake recording, these systems present an effective way of communicating the entitlement to the beneficiary that remains a critical problem despite various efforts by the Governments and other agencies. It also allows for considerable flexibility in the choice of FPS for the consumer (with sufficient prior notice) and therefore introduces an element of competition between different FPS and gives the consumer the power to move to another FPS if not satisfied with the level of service.

Information, Communication Technology Infrastructure

Information Communication Technology (ICT) infrastructure will need to be deployed to connect all the key offices of the Food Department including the Secretariat, Commissioner cell, District Offices, Teshil/Block offices and Whole Sale Points. The infrastructure should include a central department data center to host the beneficiary database and all other crucial MIS functionality needed by the Department. The central data center could be collocated with the State Data Center (SDC) being setup under the NEGAP plan and the State Wide Area Network (SWAN), also a component of the NEGAP can be leveraged to establish connectivity between the department offices.

Software should include a ration card management system, an individual beneficiary offtake analysis system, an automated allotment system and a full-featured MIS system that will cater to all needs of the Department. Appropriate mechanism to extend the computerization to the field force of the Department should be explored. This could include the use of handheld devices or the PoS for managing inspections and other data collection activity.

The Ministry of IT is setting up 100,000 Common Service Centers (CSCs) under the National E-Governance Action Plan and it is recommended that these centers be used as citizen service points for the food departments. The centers can subsequently function as citizen touch points for Grievance submission and redressal as also for services such as issue of duplicate ration cards and changes to ration cards.

Implementation Mechanism

The PDS Control order stipulates that as part of the monitoring "State Governments shall ensure monitoring of the functioning of the Public Distribution System at the fair price shop level through the computer network of the NIC installed in the District NIC centers. For this purpose computerized codes shall be issued to each FPS in the district."

The program can be implemented by the State Governments with minimal changes to the clause in the PDS control order referred above.

PDS & UID - A Synergic Partnership

The UID program will create a database of all unique residents in the country. The PDS system currently serves the largest number of residents in India and efforts are underway to improve the efficiency of the system. There are several benefits that will accrue to the PDS system and the UID program if an alignment and synergy as described above can be established.

Benefits to UIDAI

There are several benefits to the UID program if this is adopted by the PDS system. The key ones are explained below:

- **Improved Coverage** - The ration card is today the most prevalent form of identity in the rural areas. If the UID enrollment is integrated into the process of the creation of a beneficiary database for PDS, the coverage of UID improves significantly.

- **Data Updating** – Ration cards are a persistent source of citizen transactions with a monthly frequency. If there is a change in the family structure, or the family moves, the ration card is sure to be updated. At this time the data can also be updated to the UID database.

Benefits to PDS System

The PDS system stands to benefit from the legislative, technology and administrative infrastructure that are being created for the implementation of the UID program. The key ones are explained below:

- **Better Identification** – Integration with the UID program will lead to better identification of individuals and families leading to better targeting and increased transparency and therefore better functioning of the system and increased public approval.

- **Offtake Authentication** – The UID database will maintain details of the beneficiary that can be updated from multiple sources. The PDS system can use this database for authentication of beneficiaries during the offtake recording process. A mechanism of verifying the ID of the person at the time of delivery of grains will help in improving the targeting of the grains.

- **Legislative Support** - The legislative support in form of the need for submitting the UID number for several transactions will push residents to acquire a UID. The most convenience mechanism will be for residents to get a ration card and this will create a supporting environment for computerization of ration cards.

- **Technology Support** – The UID program is putting together technology specifications and infrastructure to handle enrollment, storage and identity confirmation of all Indian residents. The PDS system can leverage this and rapidly move ahead with the enrollment process.

- **Duplicate and Ghost Detection** – The UIDAI will provide duplicate detection infrastructure to the PDS program. It can also assist in the development of special tools to assist in the assessment of eligibility of applicants.

- **Domestic LPG Linkage** – The issue of domestic LPG by Oil companies can be made conditional to the production of an APL (non-kerosene) ration cards making enrollment a compulsory affair.

- **Support for PDS reform** – The UID will become an important identifier in banking services and day-to-day needs of the resident. This can support the PDS reform by as an example providing the banking account number for a family to effect direct cash transfer.

Summary

The UID program has the specific objective of creating a unique database of residents in India and will put together the best technologies and processes for this purpose. UID can share the burden of PDS reform by assisting in the positive identification of unique individuals and families. This can lead to a high-quality beneficiary database without duplicate and ghost cards, improving the targeting of benefits.

The initiatives by UID in the services space will create an ecosystem for easy implementation of PDS reforms like direct benefits transfer. The UID database can also be used by the PDS system for confirmation of offtake by the resident.

The large beneficiaries in the PDS system and the regular contact with them will provide the necessary impetus for penetration of UID across the country. The efficiency improvements in the PDS system will make it one of the best-run pro-poor schemes in the country. Together, it is a win-win for residents and the Government.

152

सत्यमेव जयते

UIDAI STRATEGY OVERVIEW

CREATING A UNIQUE IDENTITY NUMBER FOR EVERY RESIDENT IN INDIA

Unique Identification Authority of India (UIDAI)
Planning Commission, Govt. of India
April, 2010

CONTENTS

Executive Summary

Overview

In India, an inability to prove identity is one of the biggest barriers preventing the poor from accessing benefits and subsidies. Public as well as private sector agencies across the country typically require proof of identity before providing individuals with services. But till date, there remains no nationally accepted, verified identity number that both residents and agencies can use with ease and confidence.

As a result, every time an individual tries to access a benefit or service, they must undergo a full cycle of identity verification. Different service providers also often have different requirements in the documents they demand, the forms that require filling out, and the information they collect on the individual.

Such duplication of effort and 'identity silos' increase overall costs of identification, and cause extreme inconvenience to the individual. This approach is especially unfair to India's poor and underprivileged residents, who usually lack identity documentation, and find it difficult to meet the costs of multiple verification processes.

There are clearly, immense benefits from a mechanism that uniquely identifies a person, and ensures instant identity verification. The need to prove identity only once will bring down transaction costs for the poor. A clear identity number would also transform the delivery of social welfare programs by making them more inclusive of communities now cut off from such benefits due to their lack of identification. It would enable the government to shift from indirect to direct benefits, and help verify whether the intended beneficiaries actually receive funds/subsidies.

A single, universal identity number will also be transformational in eliminating fraud and duplicate identities, since individuals will no longer be able to represent

themselves differently to different agencies. This will result in significant savings to the state exchequer.

The UIDAI – evolving an approach to identity

The Government of India undertook an effort to provide a clear identity to residents first in 1993, with the issue of photo identity cards by the Election Commission. Subsequently in 2003, the Government approved the Multipurpose National Identity Card (MNIC).

The Unique Identification Authority of India (UIDAI) was established in January 2009, as an attached office to the Planning Commission. The purpose of the UIDAI is to issue a unique identification number (UID) to all Indian residents that is (a) robust enough to eliminate duplicate and fake identities, and (b) can be verified and authenticated in an easy, cost-effective way. The UIDAI's approach will keep in mind the learnings from the government's previous efforts at issuing identity.

The UIDAI will be created as a statutory body under a separate legislation to fulfill its objectives. The law will also stipulate rules, regulations, processes and protocols to be followed by different agencies partnering with the UIDAI in issuing and verifying unique identity numbers.

Features of the UIDAI model

The Unique Identification number (UID) will only provide identity: The UIDAI's purview will be limited to the issue of unique identification numbers linked to a person's demographic and biometric information. The UID will only guarantee identity, not rights, benefits or entitlements.

The UID will prove identity, not citizenship: All residents in the country can be issued a unique ID. The UID is proof of identity and does not confer citizenship.

A pro-poor approach: The UIDAI envisions full enrolment of residents, with a focus on enrolling India's poor and underprivileged communities. The Registrars that the UIDAI plans to partner with – the NREGA, RSBY, and PDS – will help bring large numbers of the poor and underprivileged into the UID system. The UID method of authentication will also improve service delivery for the poor.

Enrolment of residents with proper verification: Existing identity databases in India are fraught with problems of fraud and duplicate/ghost beneficiaries. To prevent this from seeping into the UIDAI database, the UIDAI plans to enrol residents into its database with proper verification of their demographic and biometric information. This will ensure that the data collected is clean from the start of the program.

However, much of the poor and underserved population lack identity documents and the UID may be the first form of identification they have access to. The UIDAI will ensure that the Know Your Resident (KYR) standards don't become a barrier for enrolling the poor, and will devise suitable procedures to ensure their inclusion without compromising the integrity of the data.

A partnership model: The UIDAI approach leverages the existing infrastructure of government and private agencies across India. The UIDAI will be the regulatory authority managing a Central Identities Data Repository (CIDR), which will issue UIDs, update resident information, and authenticate the identity of residents as required.

In addition, the UIDAI will partner with agencies such as central and state departments and private sector agencies who will be 'Registrars' for the UIDAI. Registrars will process UID applications, and connect to the CIDR to de-duplicate resident information and receive UID numbers. These Registrars can either be enrollers, or will appoint agencies as enrollers, who will interface with people seeking UID numbers. The Authority will also partner with service providers for authentication.

The UIDAI will emphasize a flexible model for Registrars: The Registrars will retain significant flexibility in their processes, including issuing cards, pricing, expanding KYR (Know Your Resident) verification, collecting demographic data on residents for their specific requirements,

and in authentication. The UIDAI will provide standards to enable Registrars maintain uniformity in collecting certain demographic and biometric information, and in basic KYR. These standards have been finalized by the Demographic Data Standards and Verification Procedures Committee and Biometric Standards Committees which was constituted by the UIDAI constituted.

Enrolment will not be mandated: The UIDAI approach will be a demand-driven one, where the benefits and services that are linked to the UID will ensure demand for the number. This will not however, preclude governments or Registrars from mandating enrolment.

The UIDAI will issue a number, not a card: The UIDAI's role is limited to issuing the number. This number may be printed on the document/card that is issued by the Registrar.

The number will not contain intelligence: Loading intelligence into identity numbers makes them susceptible to fraud and theft. The UID will be a random number.

The UIDAI will only collect basic information on the resident: The UIDAI will seek the following demographic and biometric information in order to issue a UID number:

- . Name
- Date of birth
- Gender
- Father's/ Husband's/ Guardian's name and UID number (optional for adult residents)
- Mother's/ Wife's/ Guardian's name and UID number (optional for adult residents)
- Introducer's name and UID number (in case of lack of documents)
- Address
- All ten fingerprints, photograph and both iris scans

Process to ensure no duplicates: Registrars will send the applicant's data to the CIDR for de-duplication. The CIDR will perform a search on key demographic fields and on the biometrics for each new enrolment, to ensure that no duplicates exist.

The incentives in the UID system are aligned towards a self-cleaning mechanism. The existing patchwork of multiple databases in India gives individuals the incentive to provide different personal information to different agencies. Since de-duplication in the UID system ensures that residents have only one chance to be in the database, individuals will provide accurate data. This incentive will become especially powerful as benefits and entitlements are linked to the UID.

Online authentication: The UIDAI will offer a strong form of online authentication, where agencies can compare demographic and biometric information of the resident with the record stored in the central database. The Authority will support Registrars and agencies in adopting the UID authentication process, and will help define the infrastructure and processes they need.

The UIDAI will not share resident data: The UIDAI envisions a balance between 'privacy and purpose' when it comes to the information it collects on residents. The agencies may store the information of residents they enrol if they are authorized to do so, but they will not have access to the information in the UID database. The UIDAI will answer requests to authenticate identity only through a 'Yes' or 'No' response

Technology will undergird the UIDAI system: Technology systems will have a major role across the UIDAI infrastructure. The UID database will be stored on a central server. Enrolment of the resident will be computerized, and information exchange between Registrars and the CIDR will be over a network. Authentication of the resident will be online. The Authority will also put systems in place for the security and safety of information.

Benefits

For residents: The UID will become the single source of identity verification. Once residents enrol, they can use the number multiple times - they would be spared the hassle of repeatedly providing supporting identity documents each time they wish to access services such as obtaining a bank account, passport, driving license, and so on.

By providing a clear proof of identity, the UID will also facilitate entry for poor and underprivileged residents into the formal banking system, and the opportunity to avail services provided by the government and the private sector. The UID will also give migrants mobility of identity.

For Registrars and enrollers: The UIDAI will only enrol residents after de-duplicating their records. This will help Registrars clean out duplicates from their databases, enabling significant efficiencies and cost savings. For Registrars focused on cost, the UIDAI's verification processes will ensure lower KYR costs. For Registrars focused on social goals, a reliable identification number will enable them to broaden their reach into groups that till now, have been difficult to authenticate. The strong authentication that the UID number offers will improve services, leading to better resident satisfaction.

For Governments: Eliminating duplication under various schemes is expected to save substantial money for the government exchequer. It will also provide governments with accurate data on residents, enable direct benefit programs, and allow government departments to coordinate investments and share information.

Revenue Model

By providing identity authentication, the UIDAI will be taking on a process that costs agencies and service providers hundreds of crores every year. The Authority will evolve suitable policies on the issue of charging a fee for its authentication services, which will offset its long-term costs. Registrars and service providers will also be able to charge for the cards they issue residents with the UID number. Such pricing will be within UIDAI guidelines.

Timelines

The UIDAI will start issuing UIDs between August 2010 and February 2011, and plans to cover 600 million people within 4 years from the start of the issuing of the first set of UIDs. This can be accelerated if more Registrars partner with the UIDAI for both enrolment and authentication. The adoption of UIDs is expected to gain momentum with time, as the number establishes itself as the most accepted identity proof in the country.

Conclusion

India will be the first country to implement a biometric-based unique ID system for its residents on such a large scale. The UID will serve as a universal proof of identity, allowing residents to prove their identity anywhere in the country. It will give the government a clear view of India's population, enabling it to target and deliver services effectively, achieve greater returns on social investments, and monitor money and resource flows across the country.

The timing of this initiative is encouraging – the creation of the UIDAI coincides with growing social investment in India, a shift in focus to direct benefits, and with the spread of IT and mobile phones, which has made the public receptive to technology-based solutions. The UIDAI is committed to making this project a success. An initiative of this magnitude will also require the active participation of central, state and local governments, as well as public and private sector agencies across the country. With their support, the project will help realize a larger vision of inclusion and development for India.

1

Introduction and historical background

A crucial factor that determines an individual's well-being in a country is whether their identity is recognized in the eyes of the government. Weak identity limits the power of the country's residents when it comes to claiming basic political and economic rights. The lack of identity is especially detrimental for the poor and the underprivileged, the people who live in India's "social, political and economic periphery". Agencies in both the public and private sector in India usually require a clear proof of identity to provide services. Since the poor often lack such documentation, they face enormous barriers in accessing benefits and subsidies.

For governments and individuals alike, strong identity for residents has real economic value. While weak identity systems cause the individual to miss out on benefits and services, it also makes it difficult for the government to account for money and resource flows across a country. In addition, it complicates government efforts to account for residents during emergencies and security threats.

However in India, the goal of issuing a universally used, unique identity number to each resident poses a significant challenge. A project of this scale has not been attempted anywhere in the world, and requires an innovative model, distinct from what we have witnessed in identity systems so far anywhere in the world.

1.1 Historical background and evolution of the UIDAI project

The Unique identification project was initially conceived by the Planning Commission as an initiative that would provide a clear and unique identity number for each resident across the country and would be used primarily as the basis for efficient delivery of welfare services. It would also act as a tool for effective monitoring of various programs and schemes of the Government.

The concept of unique identification was first discussed and worked upon since 2006 when administrative approval for the project –"Unique ID for BPL families" was given on March 3rd, 2006 by the Department of Information Technology, Ministry of Communications and Information Technology. This project was to be implemented by the NIC over a period of 12 months. Subsequently, a Processes Committee to suggest processes for updation, modification, addition and deletion of data fields from the core data base to be created under the Unique ID for BPL families Project was set up on July 3rd, 2006.

A "Strategic Vision on the UID Project" was prepared and submitted to this Committee. It envisaged the close linkage that the UID would have to the electoral database. The Committee also appreciated the need of a UID Authority to be created by an executive order under the aegis of the Planning Commission to ensure a pan-departmental and neutral identity for the Authority and at the same time enable a focused approach to attaining the goals set for the XI Plan. The Seventh

Meeting of the Process Committee on 30th August 2007 decided to furnish to the Planning Commission a detailed proposal based on the resource model for seeking its "in principle" approval.

At the same time, the Registrar General of India was engaged in the creation of the National Population Registrar and issuance of Multi-purpose National Identity Cards to citizens of India.

Therefore, it was decided, with the approval of the Prime Minister, to constitute an Empowered Group of Ministers (EGoM) to collate the two schemes – the National Population Register under the Citizenship Act, 1955 and the Unique Identification Number project of the Department of Information Technology. The EGoM was also empowered to look into the methodology and specific milestones for early and effective completion of the Project and take a final view on these. The EGoM was constituted on December 4th, 2006.

The first meeting of the EGoM was held on November 27th, 2007. It recognised the need for creating an identity related resident database, regardless of whether the database is created based on a de-novo collection of individual data or is based on already existing data such as the voter list. It also recognised that there is a crucial and imperative need to identify and establish an institutional mechanism that will "own" the database and will be responsible for its maintenance and updating on an ongoing basis, post its creation.

The second meeting of the EGoM was held on January 28th, 2008. It decided on the strategy for the collation of NPR and UID. Inter-alia, the proposal to establish UID Authority under the Planning Commission was approved.

The third meeting of the EGoM was held on August 7th, 2008. The Planning Commission had placed before the EGoM a detailed proposal for setting up the UIDAI. The meeting decided that certain issues raised by the members with relation to the UIDAI would need to be examined by an official level committee. It referred the matter to a Committee of Secretaries to examine and give its recommendations to the EGoM to facilitate a final decision.

Subsequent to the Committee of Secretaries recommendations, **the fourth meeting of the EGoM** was held on November 4th, 2008.The recommendations of the Committee of Secretaries was presented to the EGoM and the following decisions were taken:

a) Initially the UIDAI may be notified as an executive authority, and investing it with statutory authority could be taken up for consideration later at an appropriate time.

b) UIDAI may limit its activities to the creation of the initial database from the electoral roll/EPIC data. UIDAI may however additionally issue instructions to agencies that undertake creation of databases to ensure standardization of data elements.

c) UIDAI will take its own decision as to how to build the database.

d) UIDAI would be anchored in the Planning Commission for five years after which a view would be taken as to where the UIDAI would be located within Government.

e) Constitution of the UIDAI with a core team of 10 personnel at the central level and directed the Planning Commission to separately place a detailed proposal with the complete structure, rest of staff and organizational structure of UIDAI before the Cabinet Secretary for his consideration prior to seeking approval under normal procedure through the DoE/CCEA.

f) Approval to the constitution of the State UID Authorities simultaneously with the Central UIDAI with a core team of 3 personnel.

g) December 2009 was given as the target date for UID to be made available for usage by an initial set of authorized users.

h) Prior to seeking approval for the complete organizational structure and full component of staff through DoE and CCEA as per existing procedure, the Cabinet Secretary should convene a meeting to finalize the detailed organizational structure, staff and other requirements.

1.1. Subsequently, on January 22nd, 2009 the Cabinet Secretary in pursuance of the decisions of the Empowered Group of Ministers considered the proposal submitted by the Department of Information Technology regarding the governance structure and recommended that

a) The notification for constitution of the UIDAI should be issued immediately.

b) A High Level Advisory, Monitoring and Review Committee headed by Deputy Chairman, Planning Commission to be constituted to oversee the work of the authority.

c) A Member, Planning Commission or the Secretary, Planning Commission may be also assigned the task of looking after the work proposed of the Chief UID Commissioner.

d) Core Team to be put in place.

In pursuance of the Empowered group of Ministers' fourth meeting dated November 4th, 2008, the **Unique Identification Authority of India** was constituted and notified by the Planning Commission on January 28th, 2009 as an attached office under the aegis of Planning Commission with an initial core team of 115 officials. The role and responsibilities of the UIDAI was laid down in this notification. The UIDAI was given the responsibility to lay down plan and policies to implement UID scheme, and shall own and operate the UID database and be responsible for its updation and maintenance on an ongoing basis.

Subsequently on July 2nd, 2009 Shri Nandan Nilekani was appointed as the Chairman of the UIDAI. Shri Nilekani assumed charge on 23rd July, 2009 and since then the UIDAI has started functioning.

The Prime Minister's Council on UID Authority was constituted on 30th July, 2009 and its first meeting had taken place on 12th August, 2009. The Council endorsed the broad approach submitted by the UIDAI.

Subsequently, the Government constituted a **Cabinet Committee on Unique Identification**

Authority of India vide its order no 1/11/6/2009 dated 22nd October, 2009. The functions of this Committee, as per this notification are: All issues relating to the Unique Identification Authority of India including its organisation, plans, policies, programmes, schemes, funding and methodology to be adopted for achieving the objectives of that Authority.

1.2 The UIDAI approach

In 2007, the Planning Commission had recommended an approach to issuing unique identification numbers, where the enrolment into a Unique Identification (UID) database could be speeded up by using existing resident records in the databases of the Election Commission, PAN etc. This approach would speed up enrolment for those residents present in one of the aforementioned databases. These databases however, may contain inaccuracies.

The model envisioned by the Unique Identification Authority of India (UIDAI) takes into account the inputs of the Planning Commission, as well as learnings from the previous approaches to identity. The detailed approach and the model of implementation is explained in subsequent chapters.

2

The UIDAI implementation model

The model that the UIDAI envisions will have the reach and flexibility to enrol residents across the country.

The UIDAI, as a statutory body, will be responsible for creating, administering and enforcing policy. The UIDAI will prescribe guidelines on the biometric technology, the various processes around enrolment, and verification procedures to be followed to enroll into the UID system. The UIDAI will also design and create the institutional microstructure to effectively implement the policy. This will include a Central ID Data Repository (CIDR), which will manage the central system, and a network of Registrars who will establish resident touch points through Enrolling Agencies.

2.1 The Central Identities Data Repository (CIDR)

The CIDR will be the central data repository, and will function as a Managed Service Provider. It will implement the core services around the UID – it will store resident records, issue unique identification numbers, and verify, authenticate and amend resident data.

The CIDR will only hold the minimum information required to identify the resident and ensure no duplicates. This will include:

2.2 The Unique Identity Number

The Unique ID or UID will be a numeric that is unique across all 1.2 billion residents in India.

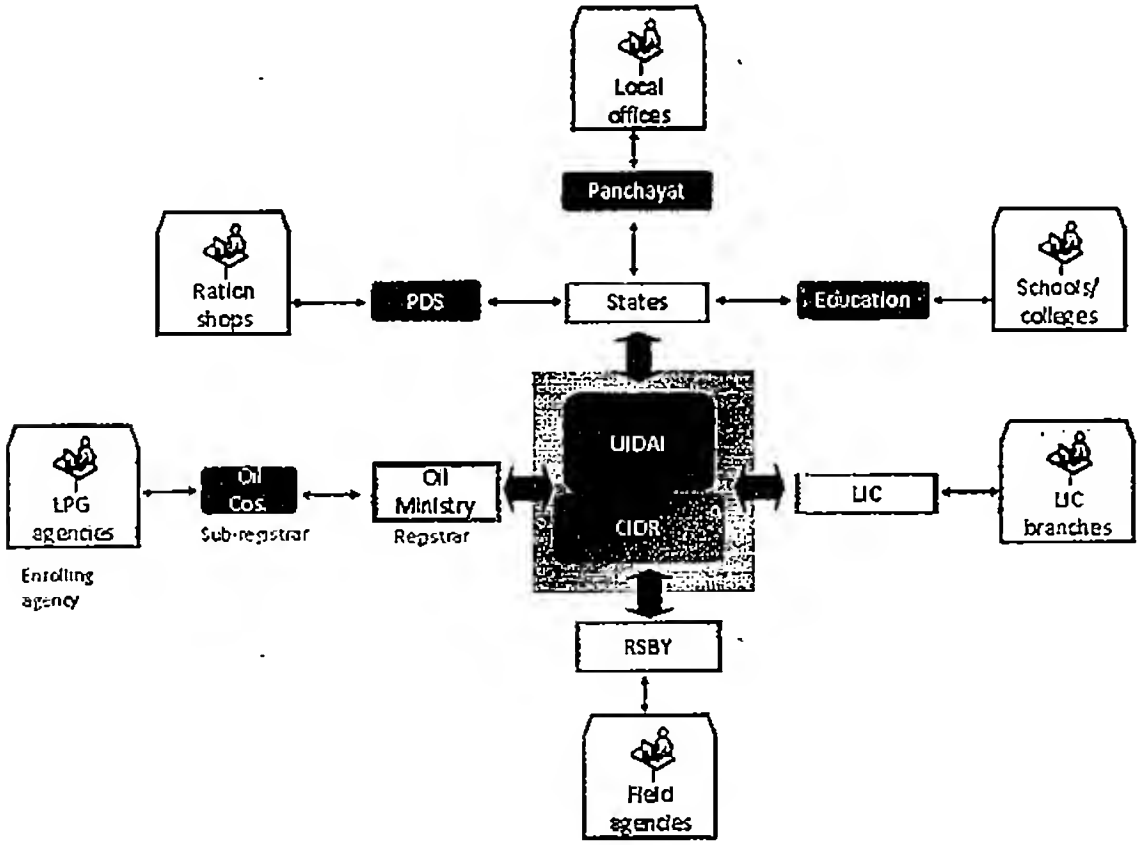
The UID number will not contain intelligence. In older identity systems, it was customary to load the ID number with information related to the date of birth, as well as the location of the person. However this makes the number susceptible to fraud and theft, and migration of the resident quickly makes location details out of date. The UID will be a random number.

The UIDAI will also be collecting the following data fields and biometrics for issuing a UID:

- Name
- Date of birth
- Gender
- Father's/ Husband's/ Guardian's name and UID (optional for adult residents)
- Mother's/ Wife's/ Guardian's name and UID (optional for adult residents)
- Introducer's name and UID (in case of lack of documents)
- Address
- All ten finger prints, photograph and both iris scans

2.3 The Unique ID agencies

The UIDAI will partner with a variety of agencies and service providers to enrol residents for UID numbers and verify their identity.



The structure of these UID agencies will be as follows:

Registrars – Registrars will be State governments or central government agencies such as the Oil Ministry and LIC. Registrars may also be private sector participants such as banks and insurance firms.

The UIDAI will enter into memorandum of understandings' (MoUs) with individual Registrars, and enable their on-boarding into the UID system. The Registrars will need to make changes to their processes to be UID-ready. The UIDAI will support them in this, and in linking to the CIDR, connecting to the UID system, and adding UID fields to their databases.

The Registrar will take on the responsibility of ensuring that clean and correct data flows into the CIDR. Their key role in the system will be in aggregating enrolments from sub-registrars and enrolling agencies and forwarding it to the CIDR. Each Registrar will adopt UIDAI standards in the technology used for biometrics, as well as in collecting and verifying resident information, and submitting to audits.

The UIDAI will also enter into agreements with some Registrars for using the CIDR solely for authentication purposes. The service providers who will adopt the UID system for identity authentication during service delivery will follow certain processes and standards, and may need to re-engineer their internal processes.

Sub-Registrars – These will be the departments/entities that report to a specific Registrar. For instance, the line departments of the state government such as the RDPR (Rural Development and Panchayati Raj) department would be sub-registrars to the state government Registrar.

Enrolling Agencies – Enrolling agencies will directly interact with and enrol residents into the CIDR. For example, the hospital where a baby is born would be the 'enrolling agency' for the baby's UID, and would report to the municipality sub-registrar.

Outreach Groups – The UIDAI along with the Registrars will also partner with civil society groups and community networks which will promote the UID number and provide information on enrolment for hard to reach and marginalised populations.

2.4 Setting standards on demographic data and biometrics

The UIDAI's approach relies on the uniformity of standards in certain vital areas of operation. The Demographic data fields and verification procedure in the UID system as well as the Biometric standards to be utilized need to be standardized across the country and across the various registrars in the UID system. This is a sine qua non for the operability of the system. Hence, the UIDAI established two Committees to look into the issue of standards.

Committee on Demographic Data Standards and Verification Procedures

The UIDAI had constituted a Committee headed by Mr. N. Vittal, former CVC on 9th October 2009 to go into the question as to what demographic details should be collected from the residents for assigning of unique IDs. The Committee was also to go into the question as to what should be the process of verification of the residents at the time of their enrolment into the UID system. The mandate of the Committee was crucial because it is necessary to ensure that the integrity and correctness of the data is not compromised while ensuring that the process of verification is non-harassing to individuals. The Committee was mandated to give its report within 90 days of its constitution. However, it submitted its report on 9th December 2009, well before the ninety days' period given to it. The Report of the Committee has been accepted by the Authority. The Committee recommended the following data fields : Name, Date of birth, Gender, Father's/ Husband's/ Guardian's name and UID (optional for adult residents), Mother's/ Wife's/ Guardian's name and UID (optional for adult residents), Introducer's name and UID (in case of lack of documents) and Address. It has also specified the verification process which broadly falls into three categories (i) Document-based, (ii) Introducer-based (in case of lack of documents) and (iii) Community-based verifications, a process which will be followed during the creation of NPR. The Report of the Vittal Committee is available at www.uidai.gov.in

Committee on Biometric Standards

As biometric attributes of the residents are going to be used as the basic signature for de-duplication and to ensure uniqueness, it is necessary to go into the question as to what should be the type and specifications of biometrics to be collected at the time of enrolment. Therefore, a Biometrics Standards Committee, under the Chairmanship of the Director General of NIC, Dr. BK Gairola was constituted by the Authority on 29th September, 2009. This Committee was also expected to give its report within 90 days of its constitution. The Report was submitted on 7th January, 2010. The UIDAI has examined their Report and has accepted the standards for various biometric attributes as recommended by the committee as also various other recommendations related to collection of biometrics and their quality. The UIDAI has also decided that the face, all ten finger prints and both iris scans should be collected at the time of capturing the demographic and biometric details of a resident. This will be able to ensure uniqueness of the IDs at a scale of 1.2 billion residents. The report of the biometric committee is also available at www.uidai.gov.in

The UIDAI was declared as an Apex body to set standards in the areas of biometric and demographic data standards by the Prime Minister's Council of UIDAI. Now that both these standards have been finalized by the UIDAI, these standards/specifications, processes and systems will be used by all the registrars to for enrolment of the residents into the UID system.

3

Enrolment into the UID system

A critical aspect of the UID enrolment process is that enrolment will not be through a mandate, but will be demand driven. The momentum for the UID will come from residents enrolling in order to access the benefits and services associated with it.

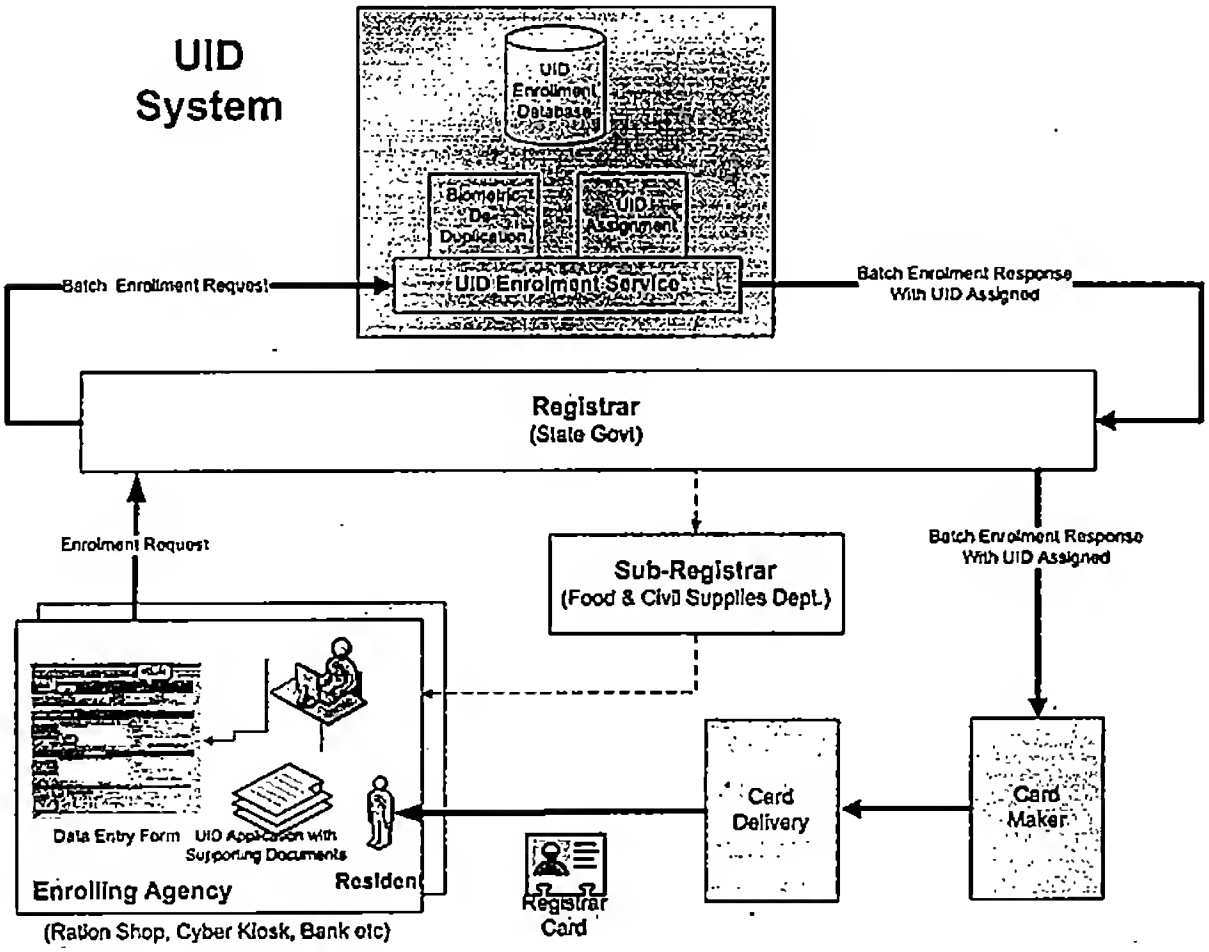
The basic advantage of the UID that can drive this demand, which will be communicated while promoting enrolment, is that the UID will be one number, which can be used to prove identity for life. Once the resident gets the unique ID, it may be accepted as identity proof across service providers.

3.1 The enrolment process

The enrolment process for the UID number will begin with a resident submitting his/her information to the enrolling agency with supporting documents. This information will be verified according to the prescribed verification procedure as per the DDSVP Committee Report. To make sure the poor are not excluded, the UIDAI has prescribed guidelines for applicants without documents.

Once the enroller verifies the resident's information, it will submit the application request – either singly or in batches – through the Registrar to the CIDR. The CIDR will then run a de-duplication check, comparing the resident's biometric and demographic information to the records in the database to ensure that the resident is not already enrolled.

Since de-duplication also compares biometric records, it would catch individuals enrolling with a different set of demographic details. The fact that the UID system is both de-duplicated and universal will discourage residents from giving incorrect data at the time of enrolment.



Issuing the UID number

Once the UID number is assigned, the UIDAI will forward the resident a letter which contains his/her registered demographic and biometric details. This letter may also have a tearaway portion which has the UID number, name, photograph and a 2D barcode of the finger print minutiae digest. If there are any mistakes in the demographic details, the resident can contact the relevant Registrar/enrolling agency as per a prescribed procedure.

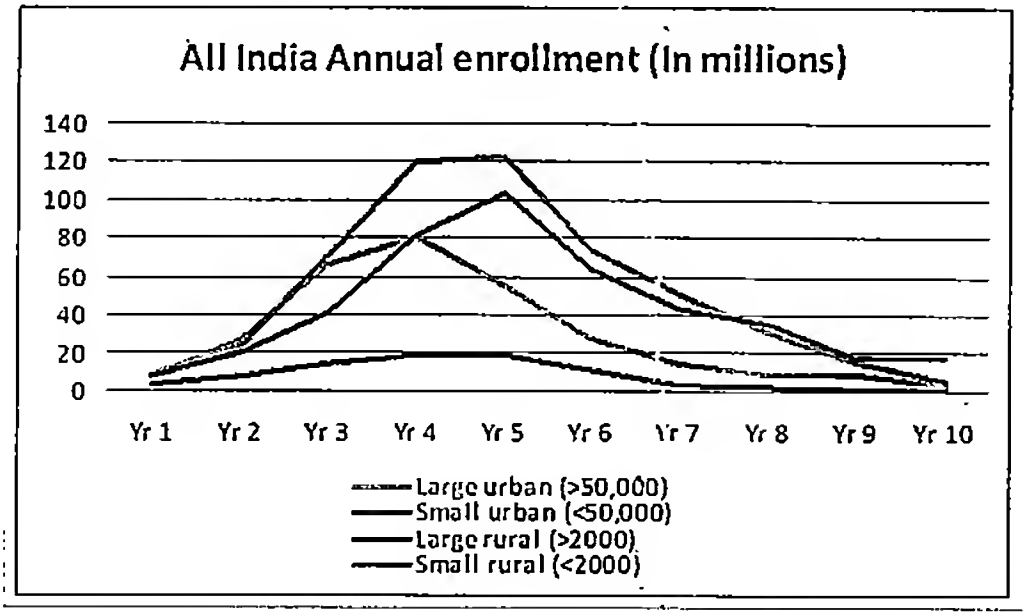
If the Registrar issues a card to the resident, the UIDAI will recommend that the card contain the UID number, name and photograph. They will be free to add any more information related to their services (such as Customer ID by bank). They will also be free to print/ store the biometric collected from the applicant on the issued card. If more registrars store such biometric information in a single card format, the cards will become interoperable for offline verification. But the UIDAI will not insist on, audit or enforce this.

All data entry that the enrolling agencies take up on behalf of the Registrars will be done in English. It can then be converted into the local language using standard transliteration software, and verified for accuracy by the Registrar. The letter the UIDAI sends the resident will consequently

contain all demographic details in English as well as the local language of the state in which the resident resides. In this regard, the UIDAI will follow the precedent set by the Election Commission of India.

3.2 Enrolment strategy in rural and urban India

The approach of the UIDAI to enrolment will be a pro-rural/pro-poor one. The Registrars targeted for rural India – the NREGA, PDS, Social security pensions - will be government agencies with large rural networks and significant bases among the poor. As a result, the UIDAI expects initial enrolment to be fairly rapid in both large and small rural areas.



The enrolment strategy for urban India will include organizations which dominate services for urban residents, such as LIC and Passports. The table below summarizes the Registrars who are

UID Registrar	Primary Access[1]	Additional Acces[2]	Potential Overlap	Effective Enrolment
	Crore Residents			
LPG (Oil PSU)	8.4[3]	16.8[4]	20%	20.2
LIC (Life Insurance)	13.5	13.5	50%	13.5
PAN Cards	4.0	-	75%	1.0
Passports	6.0	-	80%	1.2
Urban Enrolment				35.9
Lic (Life Insurance)	3.5	3.5	90%	0.7
NREGA	10.0	20.0	10%	27.0
BPL Ration Cards	7.0	21.0	60%	11.2
State BPL/APL	15.0	45.0	50%	30.0
Old Age Pensioners	1.5	1.0	70%	0.8
Women/Child Welfare	1.0	2.0	70%	0.9
Social Welfare	1.0	2.0	70%	0.9
RSBY	0.5	1.0	70%	0.5
Rural Enrolment				72.0
Total Enrolment				107.9

In addition to these enrollers, the UIDAI will also partner with the Registrar General of India (RGI) – who will prepare the National Population Register through the Census 2011 – to reach as many residents as possible and enrol them into the UID database. This may require incorporating some additional procedures into the RGI data collection mechanism, in order to make it UID-ready.

3.3 A focused effort to enrol the poor and hard to reach groups

While the UIDAI intends to target Registrars that have large networks among the poor and rural communities in India, it will also emphasize multiple approaches to reach specific, frequently marginalized groups. .

[1]These are residents who are part of the Registrar's customer / subsidiary beneficiary database and can be mandated to provide their UID

[2]The residents under additional access are family members who can be easily covered while enrolling the primary residents. These can be all family members in the case of LPG connections and the nominees in case of LIC Policies.

[3]The total number of gas connections is 10.51 crores, and this estimates that there are 20% ineligible connections

[4]Assuming there are an average of three members in each family having a gas connection from an Oil PSU

Urban Poor

The urban poor are among the most ignored and disadvantaged people in India. The main challenges in enrolment here exist because this group consists mainly of migrant workers with temporary or seasonal jobs. The following may be ways to get them enrolled into the UID system.

Co-resident enrolment: Many of India's urban poor work as drivers, maids, or as workers associated with a family or a business. One approach to reach them could be for the head of the family or business to enable these members (who are co-residents/co-workers) to get enrolled into the UID with the same address proof the business or family uses. There can be a host of financial incentives offered to enrol such co-residents.

Financial institutions: The urban poor often borrow from micro-finance institutions and other sources and these could serve as enrolment points for them. There are established chit funds that can also act as enrolment points for the UID to improve coverage.

NGOs and Non-profits: There are several established non-profits working in urban slums in education, healthcare and social empowerment. They can be used to educate the poor on the benefits of the UID, for actual enrolment and to help endorse identity for people who lack documentation.

Children

India is a young country with over 400 million residents below the age of 18. While family-based government schemes will as Registrars, help enrol children, this population may need to be specifically targeted.

ICDS: ICDS is one of the world's largest integrated early childhood programs, with over 40,000 centers nationwide. The program covers over 5 million expectant and nursing mothers and 25 million children under the age of six. These centers can be information or enrolment points for non-school going children.

School admission: It may be mandated that at the time of joining school (first standard) it is necessary for children to have a UID or to enrol for one. This way the child can be tracked for progress and targeted for direct benefits.

The SSA program could also help enrol children in the 6-14 age group into the UID, which would also enable better child tracking and improvements in the mid-day meal schemes.

For children, the advantages from the UID would be significant. Child-related programs in India have relied on often inaccurate, aggregate data at school/cluster/block levels, making these programs ineffective. The concept of Universal Child Tracking – the ability to track every child and ensure their all round development – is gaining ground. An accurate database of children with UIDs would be immensely beneficial to programs within the Women and Child welfare as well as the Education departments, which track development in anganwadis and progress of children in government schools, and work to eliminate child labor.

Women

Apart from enrollers that are family-based government services in both urban and rural India such as PDS, RSBY etc, there needs to be a strategy to cover women outside this net:

Financial institutions: Robust collectives of women exist within micro-finance institutions and self-help groups across the country. These would be important enrolment points for women.

Organizations like Mahila Samakhya in the 9 states of Karnataka, Kerala, Andhra Pradesh, Gujarat, Uttar Pradesh, Uttar Khand, Assam and Jharkhand. They work in several thousand villages to help women and can act as touch points for education or enrolment of women.

The National Commission for Women: This is the apex national level organization of India for protecting and promoting the interests of women. They have a massive outreach program that can reach out to disadvantaged women and get them to enrol. The UID can subsequently be used as a unique handle for a variety of services to be rendered to these women.

Differently-abled people

It is estimated that India has over 60 million differently-abled people, and identity for this population is a massive challenge. The Disability Act of 1995 mandates a certain percentage of employment for the differently-abled, but without the clear identification of such individuals, it is difficult to enforce the law. There is an obvious incentive for organizations like National Center for Promotion of Employment for Disabled People (NCPEDP) to promote the UID, and enable residents with disability to register for a range of benefits. The NGOs and rights groups associated with NCPEDP would also be good mechanisms to reach out to this section of the population.

Tribals

India has a significant tribal population of approximately 90 million tribals, mostly concentrated along a few states. The Government has many programs for the 697 notified tribes, which can be used for enrolment and information dissemination. In addition, NGOs and governments in states with high tribal populations can be Registrars for tribal groups.

The above mentioned approaches are merely indicative of the strategy that the UIDAI will follow to reach marginalized groups. In addition, the UIDAI will reach out to other marginalized groups such as homeless people, individuals in shelter homes, remand homes, asylums, etc.

Civil Society Outreach strategy

3.4 Enrolment costs

Enrolment costs can be thought of in two ways. One will be the cost to the enrolling agencies/Registrars for carrying out the enrolment process. The other costs will be to the residents to come to the enrolment stations. Poor may have to forego their wages for a day and also spend some travel costs to travel to the enrolment stations The enrolment strategy will explore the

possibility of various mechanisms for funding the enrolment costs. The Registrars have the option here of charging for the cards they issue residents to offset enrolment costs. The UIDAI may issue guidelines around such pricing.

3.5 Ensuring clean enrolment data from Registrars

The UIDAI will periodically carry out a process audit of the information that comes in from the Registrars, to ensure data quality and that agencies are following guidelines recommended by the UIDAI. The audit would be on a random sample of residents, carried out either directly by the Authority or through appointed agencies. The audit might focus on:

Verification against scanned documents – The data contained in the resident records will be verified against the scanned documents.

Physical document verification – The physical documents that are held by the Registrar will be validated against the electronic copies.

Periodic process audits- Periodic audits will be carried out to at the enrolment sites, of the processes and software.

3.6 Updating UID details

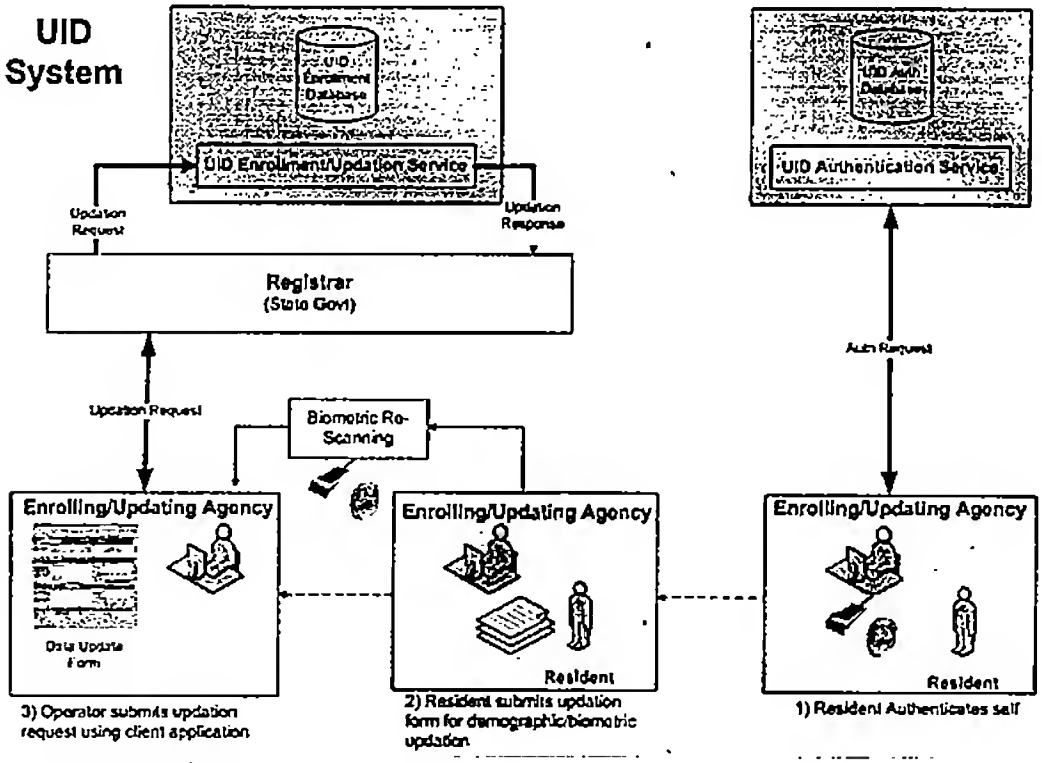
Updating information with the UIDAI

The UID number is a lifetime number, but the biometric information contained in the central database will have to be regularly updated. Children may have to update their biometric information every five years, while adults update their information every ten years.

From time to time, the demographic information that the CIDR holds on the resident may also become outdated. Fields that are susceptible to change could be the 'present address' field, as well as the resident's name (after marriage). There might also be an error in the fields that occurred during enrolment into the UID.

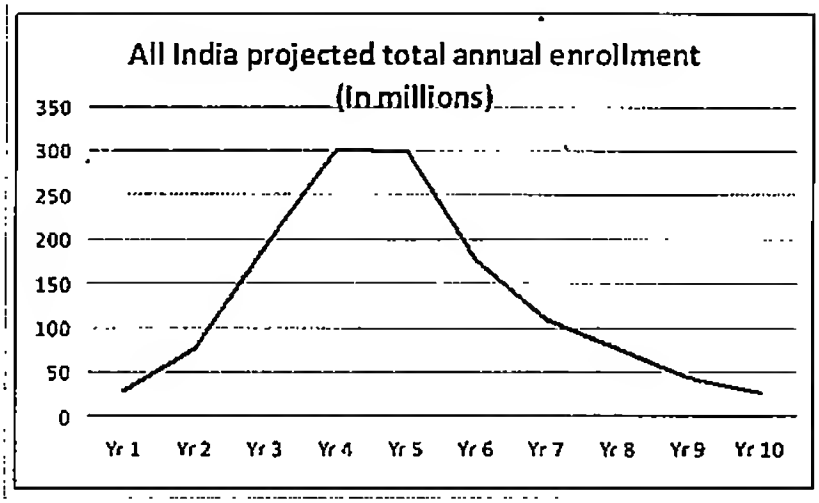
If a service provider authenticating or enrolling a resident finds, through its KYR process that the information provided by the resident (address, name, etc.) does not match with the UID record, or that the biometrics need to be renewed, it can ask the resident to update their information in the UID database. The service provider may make the update a condition for the resident to receive the service/benefit.

Enrolling agencies and Registrars can serve as points where the resident can update their UID fields. The resident will have to submit their new information at these updation points with the required documentary evidence. This may also include a biometric authentication prior to processing the request.



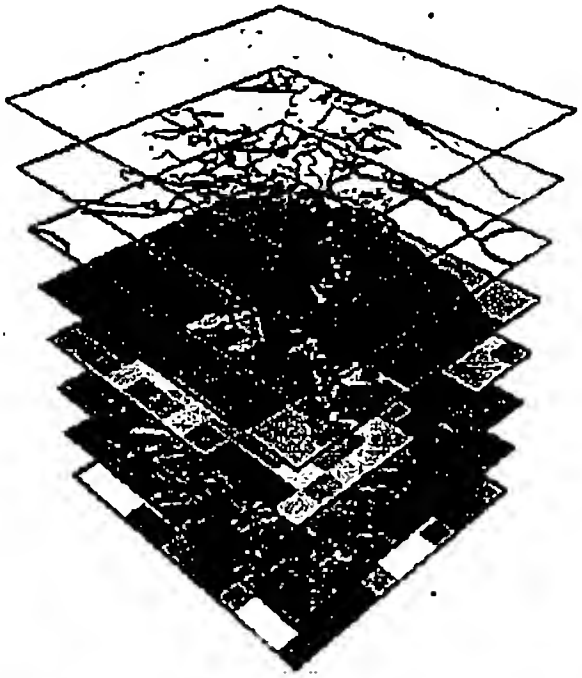
3.7 Reaching critical mass in enrolments

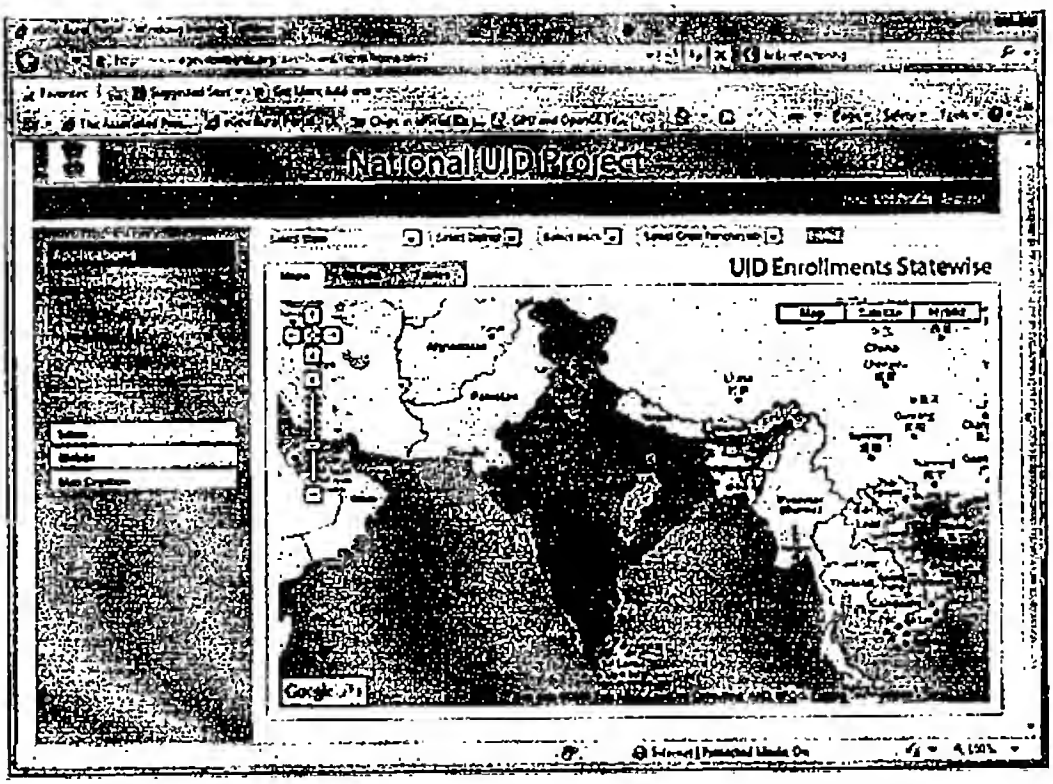
The Authority expects to start issuing the first set of UIDs between August 2010 to February 2011, and enrolment for the UID number is expected to reach a critical mass of around 200 million residents in two to three years. Until this point, the UIDAI will have to focus on generating demand from both Registrars and residents. However, once the critical mass is achieved, it will generate a network effect that drives demand and accelerates adoption among service providers and residents. And as more service providers across the country require the UID to dispense their services and benefits, adoption will ramp up rapidly. In four years, the UIDAI estimates that it will issue 600 million UID numbers.



3.8 Tracking enrolments across the country

The UIDAI will employ a GIS internet-based visual reporting system to track enrolment trends and patterns across India, as the project is rolled out across various Registrars and states.





The GIS system will show all UID enrolments by state, as well as by Registrar. The system will also be able to drill down within states and into districts.

3.9 Reaching a sustainable, steady-state in enrolment

A challenge for full enrolment is registering the approximately 60,000 babies that are born in the country every day. Over the next several years, the UIDAI expects to enrol close to the entire Indian population. Once that goal is achieved, enrolment will reach a steady state, where only births (and deaths) as well as immigrants need to be recorded.

There are however, some challenges in registering new births. First, since their biometrics is not stable, they have to be re-scanned at a later age. Second, names are often not given in India at the time of birth registration.

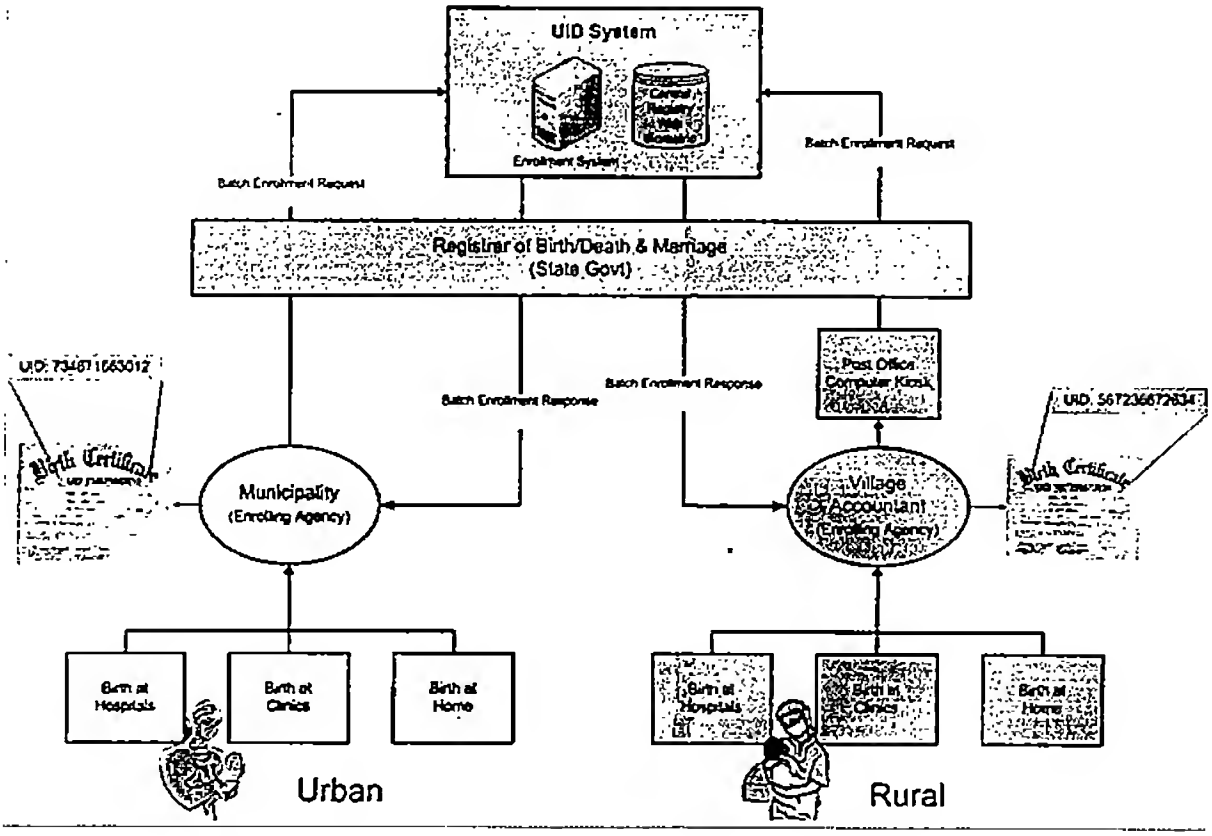
The UID in the birth certificate

One way to ensure that the UID number is used by all government and private agencies is by inserting it into the birth certificate of the infant. Since the birth certificate is the original identity document, it is likely that this number will then persist as the key identifier through the individual's various life events, such as joining school, immunizations, voting etc.

Since the name is a mandatory field in the UID database, it is essential that the child be given a name before applying for the UID number. This would ensure that the UID can also be allotted at birth.

In the case of urban births, the municipality will be the enrolling authority and the UID Registrar can be the 'Registrar of Births, Deaths and Marriage' at the state level.

In rural areas, births take place at district or block level hospitals, in health care centers and at homes in the village. The village accountant is the Registrar of rural births, and he/she also issues the birth certificate and updates the information through an enrolling agency.



Biometrics and infants

The recording of unique individual biometrics in the UID database is a challenging one for infant records. The solution to this is to record the UID and biometric of the parents in the child's record.

The child's biometrics need to be taken at around 5 years of age, and updated in the UID system every 5 years until the age of 18. This will be enforced by an expiry date attached to the UID number, which will become invalid after that date. Until the time the biometric of the child stabilizes, any one of the parents/guardian will need to provide their biometric information for authentication.

Recording deaths in the UID system

It is also necessary to record deaths in the country, and the birth and death registration act provides for such registration. The same institutions that record births can be in charge of updating deaths in the UID system. The UID system will not remove a record upon the person's death; it will simply mark it as 'deceased' and hence will render it inactive for the purposes of authentication.

4

Ensuring strong authentication, and what it means for the UIDAI

The real test of reliability for the UID system will be during identity authentication. Confirming 'you are who you say you are' remains the primary, often elusive goal of all identity systems.

The UIDAI approach – which will be online authentication, with biometric check – creates a very strong authentication system, and gives the UIDAI significant ability to confirm an individual's identity. The UIDAI will support the Registrars in building the infrastructure and systems necessary to authenticate residents in different parts of the country. This will be especially critical for Registrars working in rural areas and among the poor.

4.1 Enabling UID adoption for authentication

The speed of UID adoption in India depends on whether the number can help in eliminating poverty and marginalization, and in enabling greater transparency and efficiency in service delivery. If it succeeds in these goals, the number will become indispensible for residents in accessing services.

While the UID can provide the strongest form of pre-verification and identity authentication in the country, it cannot ensure that targeted benefit programs reach intended beneficiaries. The pro-poor impact of the UID, consequently, will not gain traction unless there is a mechanism to link the UID process with actual service delivery.

A clear adoption process can overcome this gap by helping introduce the UID method of authentication at every point of service delivery. To ensure this, the UIDAI will not only work with Registrars who do enrolment, but also with non-enrolling, service delivery agencies. Such agencies involved in the delivery of services and benefits will be encouraged to partner with the UIDAI for authentication. Once they authenticate a resident's identity against the UID database every time they carry out a service transaction, they will be able to deliver services far more effectively.

In order to accommodate this authentication, agencies may need to re-engineer their business processes to be UID-enabled. The most basic requirement for change will be in incorporating the UID method of authentication into their systems. Agencies will have to adhere to norms and procedures specified by the UIDAI for fingerprint capture and verification, and introduce a robust biometric authentication process at every point of sale.

There is tremendous value to be gained from widespread adoption of the UID for authentication, especially for residents. While enrolment in the UID database will ensure that residents are not denied access to fundamental services and rights because they cannot present positive proof of identity, adoption in authentication could go one step further, and ensure that residents

consistently receive these services. This can include a wide range of benefits such as education, health coverage, old-age pensions and subsidized food grains, thereby fulfilling the UIDAI's pro poor agenda.

The UIDAI is only in the identity domain. The responsibility of tracking beneficiaries and the governance of service delivery will continue to remain with the respective agencies – the job of tracking distribution of food grains among BPL families for example, will remain with the state PDS department. The adoption of the UID will only ensure that the uniqueness and singularity of each resident is established and authenticated, thereby promoting equitable access to social services.

The adoption of the UID during authentication will also have a direct correlation with subsequent enrolment. Greater enrolment comes from the value a resident derives from the UID, which in turn depends on the rate of adoption. There is a positive cycle here, created from the relationship between adoption and enrolment – the greater the adoption, the faster the enrolment and vice versa. The twin approaches of enrolment and adoption will result in greater influence and traction for the UID among residents in the country, and establish the UIDAI as the only genuine identity authenticator in India.

4.2 Types of authentication

There are multiple forms of authentication that the UID authority can offer. Certain types of authentication would have low to medium assurance if there is the possibility that the card is forged. Here we summarize the main forms of authentication, depending on the situation and equipment available.

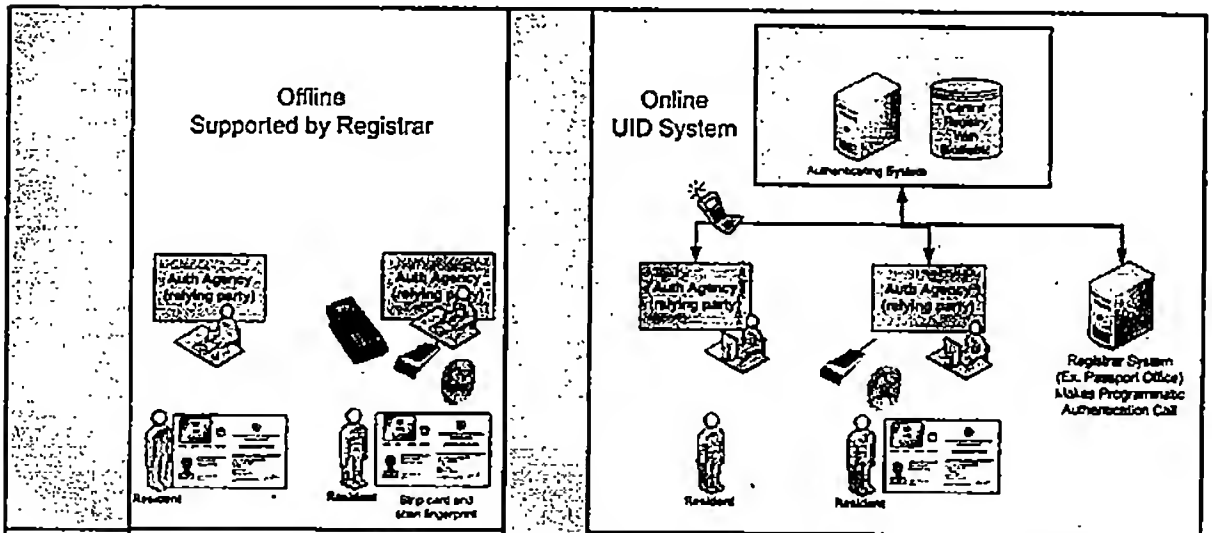
Online authentication is supported by the UID system. This can include

- Online demographic authentication where the authenticating agency compares the UID number and demographic information of the UID holder to the information stored in the UID database. The assurance level here is medium.
- Online biometric authentication where the biometrics of the UID holder, his UID and key demographic details are compared to the details in the CIDR. The assurance level in this case is high.
- Online demographic/biometric authentication with API where the Registrar's backend system makes a programmatic call to the authentication APIs exposed by the UID system to perform authentication. The assurance level here may be medium-high depending on whether the check used demographic or biometric inputs.

Offline authentication may be supported by the Registrar, and does not use the authenticating service provided by the UIDAI. This may come in two forms:

- Photo match authentication where the photo on the card is compared with the cardholder. This is the most basic form of authentication. The assurance level here is low.

- Offline biometric authentication compares the scanned fingerprint of the cardholder to the biometric stored on the Registrar-issued card. The assurance level here is medium.



	Offline		Online		
Auth Levels	Compare photo on card with card holder	Compare biometric on card with finger scan	Compare UID and demographic data online	Compare biometric on server against finger scan	Programmatic demo/bio Auth using APIs
Method	Photo Match	Biometric Auth	Demographic Auth	Biometric Auth	Demo/Bio Auth
Assurance	Low	Medium	Medium	High	Medium/High

4.3 Authentication and the UIDAI revenue model

The ability of the UIDAI to offer agencies across the country strong, reliable authentication is the key to its sustainability. The UIDAI will offer resident authentication services for a fee to governments and private sector firms.

The agencies which request a resident authentication service will have to be registered with the UIDAI and follow strict guidelines in using the service as well as in managing resident information.

Basic identity confirmation

Basic identity confirmation from the UIDAI would be free. In this transaction, the authenticator will provide the UID number, name and one other parameter such as date of birth of the person, and the central database will confirm the identity as a 'Yes' or 'No' response.

This type of transaction will be carried out in large numbers and will need quick response times.

Chargeable authentication services can be of two types:

Address verification

For security purposes, government agencies as well as private sector firms require address proof

from Indian residents before providing them with benefits and services. However, agencies often complain of the difficulty of address verification "you try to verify an address in India, and you enter a labyrinth". The service provider usually verifies address through a physical visit, as well as an enquiry to confirm the other information provided. This process is expensive and costs between Rs. 100 and Rs. 500 per verification.

The address authentication service the UIDAI will offer these entities would consequently be a valuable one. In the proposed transaction with the UID Authority, the agency will submit the UID, name and address of the resident to the CIDR, which will confirm the address. As a result, the agency will not have to do physical address verification.

Biometrics confirmation

Services such as issuing a credit card or granting a loan need the confirmation of the resident's identity. This process for the resident involves the submission of photographs and other documentation confirming their identity. In the proposed transaction with the UID Authority, the agency can send the scanned photograph or fingerprint (based on the security level required) together with other demographic details to confirm the identity of the person.

Revenue projections from authentication services

The following revenue model for the UIDAI is an illustrative one. It has been designed while keeping in mind the value the agency requesting authentication would derive from the service. The table below summarizes the kind of transaction, potential user agencies and the proposed transaction fee. Government agencies could be provided these services from the UIDAI at a subsidized rate.

Sl.	Transaction Type	Transaction Fee	Potential User Agencies
1	Basic ID Confirmation	Free	Airlines during passenger check-in
2	Address Verification	Rs. 5	Banks for account opening
3	Biometrics Confirmation	Rs. 10	Credit cards issue process

The authentication service from the UIDAI can begin after the initial bulk on-boarding of Registrars. The revenue estimates for the UIDAI below are based on the current expenditure of various agencies on KYR processes, which would be replaced by the Authority's authentication services. It also takes into account expected growth in demand for mobile connections, bank accounts, etc.

UID Revenue Projection (Steady State Estimates)	Transaction Type	
	Address	Biometrics
New Mobile Connections	19.59	-
PAN Cards	-	1.20
Gas Connections by PSU	-	1.50
Passports	0.06	-
LIC New Policies	-	10.16
Credit Cards	0.70	-
Bank Accounts	11.55	-
Airline Check-in	-	-
Projected Total Transactions	31.91	12.86
Proposed Transaction Rate	5	10
Transaction Revenue	159.55	128.60
Estimated total annual revenue at steady state (Rs. Crores)		288.15

5

Legal Framework

The Constitution of India, through the Directive Principles of State Policy[5] mandates that the state shall strive to minimize inequalities of income and endeavor to eliminate inequalities in status amongst individuals. The objective of the UIDAI is to solve the key problem of identity that individuals face and enable better and efficient delivery of services to the poor and marginalized so as to eliminate inequalities of income and status. It is therefore, imperative to have a proper legal structure in place to ensure the smooth functioning of the UIDAI. This section provides an overview of the legal and policy framework.

The Unique Identification Authority of India (UIDAI) will be set up as a statutory body by an Act of Parliament. The UIDAI will be authorized:

- To collect the following identity information from any person voluntarily seeking a unique identity number:
  - Name
  - Date of Birth
  - Gender
  - Father's name and UID number
  - Mother's name and UID number
  - Address
  - All ten finger prints, photograph and both iris scans

The law will contain a prescription against collecting any other information than the information permitted, with specific prohibitions against collection of information regarding religion, race, ethnicity, caste and other similar matters, and for the facilitation of analysis of the data for anyone or to engage in profiling or any similar activity.

- To issue a unique identity number to the person who has provided the necessary information and fulfilled the requirements as laid down in rules prescribed by the UIDAI.

Art.38 [5](1) The State shall strive to promote the welfare of the people by securing and protecting as effectively as it may a social order in which justice, social, economic and political, shall inform all the institutions of the national life.

(2) The State shall, in particular, strive to minimise the inequalities in income, and endeavour to eliminate inequalities in status, facilities and opportunities, not only amongst individuals but also amongst groups of people residing in different areas or engaged in different vocations.

- To verify the identity of any person at the time of the provision of information, the issuance of a unique identity number or at any other time per the UIDAI database or other possible means, as laid down in rules prescribed by the UIDAI.
- To permit the UIDAI to set up or facilitate the infrastructure by which third parties can authenticate the identity of persons who have provided information to the UIDAI and the circumstances and conditions they can seek such verification. The information on the database will be used only to authenticate identity.
- To establish or appoint a Central ID Data Repository (CIDR) for the purposes of collecting, managing and securing the database and to outsource any such functions.
- To permit the appointment of Registrars in accordance with criteria laid down by the UIDAI to enrol people that seek unique identity numbers directly or indirectly through enrolling agencies.
- To allow for the appointment of other service providers in accordance with criteria laid down by the UIDAI, as the UIDAI may deem fit to further its objectives and to ensure efficiency.
- To call for information and records, conduct inspections, inquiries and audit of the CIDR, Registrars, enrolling agencies and service providers..
- To enter into all necessary contracts and arrangements in order to fulfill the objectives of the UIDAI.
- To set up mechanisms for grievance redressal for the public
- To set up a monitoring framework to improve implementation, create safeguards as required and study the impact of the UID
- To hire the necessary technical and professional personnel necessary for executing the mandate and fulfill the objectives of the UIDAI.

The law will also contain

- Penal provisions against persons employed by, or associated directly or indirectly with, the CIDR, Registrars, enrolling agencies and other service providers for failing to comply with the directions issued under the Act
- Penal provisions against persons employed by, or associated directly or indirectly with the UIDAI, CIDR, Registrars, enrolling agencies and other service providers for breach of certain key sections of the legislation – including the specific prohibitions on profiling, the disclosure of information and maintenance of confidentiality etc.
- Penal provision for persons who intentionally or fraudulently provide wrong information, attempt to obtain a second unique identity number, steal the identity of any living or dead

person, etc. In this context, there will be no liability on the part of the UIDAI or persons employed by, or associated directly or indirectly with the UIDAI, CIDR, Registrars, enrolling agencies and other service providers for providing a unique identity number to a person who intentionally or fraudulently obtains such number.

Protecting privacy and confidentiality

The information that the UIDAI is seeking is already available with several agencies (public and private) in the country, the additional information being sought by the UIDAI are the finger prints and iris scans. However, the UIDAI recognizes that the right of privacy must be protected, and that people are sensitive to the idea of giving out their personal information, particularly the idea of information being stored in a central database to be used for authentication. UIDAI will protect the right to privacy of the person seeking the unique identity number. The information on the database will be used only to authenticate identity. Necessary provisions would be in place to address the issues of privacy and confidentiality.

Offences under the UIDAI Act

The UID database will be susceptible to attacks and leaks at various levels. The UIDAI must have enough teeth to be able to address and deal with these issues effectively. It will be an offence under the UIDAI Act to engage in the following activities:

- Unauthorized disclosure of information by anyone in the UIDAI, Registrar or the Enrolling agency
- Disclosure of information violating the protocols set in place by the UIDAI
- Sharing any of the data on the database with anyone.
- Engaging in or facilitating analysis of the data for anyone.
- Engaging in or facilitating profiling of any nature for anyone or providing information for profiling of any nature for anyone.
- All offences under the Information Technology Act shall be deemed to be offences under the UIDAI if directed against the UIDAI or its database.

6

Data Security and Fraud

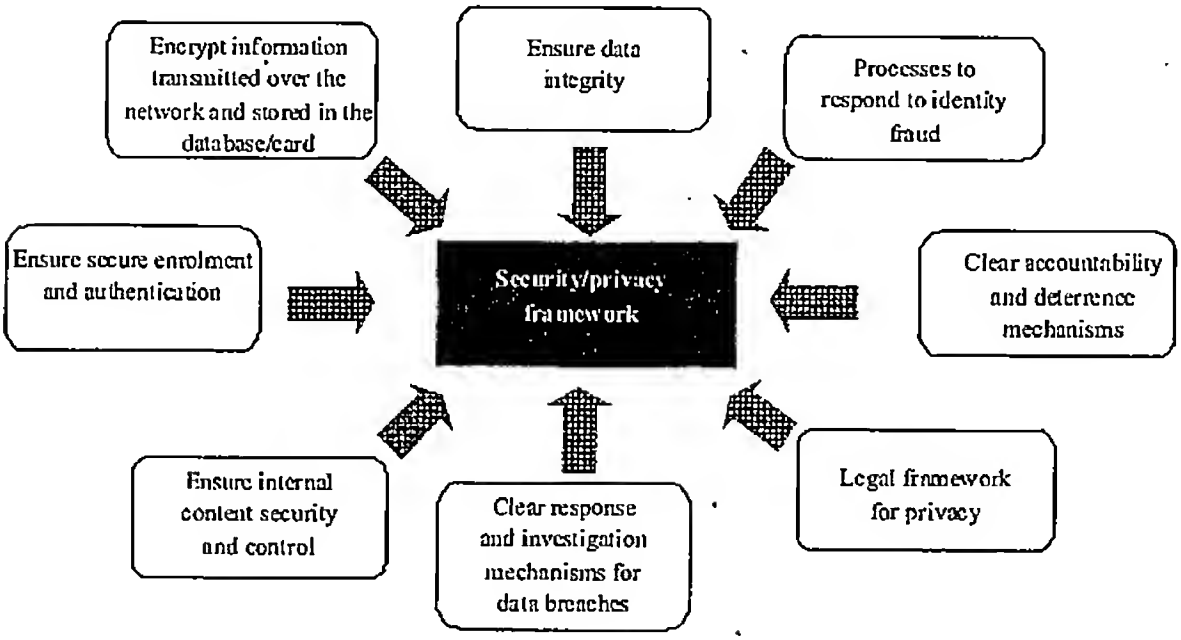
6.1 Protecting personal information of residents

Even as the UIDAI stores resident information and confirms identity to authenticating agencies, it will have to ensure the security and privacy of such information.

By linking an individual's personal, identifying information to a UID, the UIDAI will be creating a transaction identity for each resident that is both verified and reliable. This means that the resident's identity will possess value, and enable the transfer of money and resources.

The UIDAI envisions storing basic personal information, as well as certain biometrics. However, limiting its scope to this, and not linking this information to financial/other details does not make the resident records in the database non-sensitive. Biometric information for example, is often linked to banking, social security and passport records. Basic personal information such as date of birth is used to verify owners of credit card/bank accounts and online accounts. Such information will therefore, have to be protected. Loss of this information risks the resident's financial and other assets, as well as reputation, when the resident is a victim of identity theft.

In the federated system that the UIDAI envisions, we must consequently have processes in place to ensure a fair level of data security.



6.2 Fraud scenarios

The Authority will concern itself only with identity fraud, which is distinct from document fraud. Document fraud the use of counterfeited/misleading documents to enter incorrect personal information will be the responsibility of the Registrar enrolling the resident. The Authority will have clear response mechanisms in place for identity fraud, where an individual deliberately impersonates someone else, either real or fictitious.

Since the CIDR will store the biometric of residents, identity fraud will be easier to control. The only form of fraud that may go undetected in the UID system is if a person registers his/her details and biometrics under an entirely different name, with forged supporting documents. However, the person will have to exist under this name across systems, in the lifetime of his/her interaction with the government, private agencies and service providers. Such instances are therefore, likely to be rare.

Some of the potential fraud scenarios are:

Scenario	Response
Person applies for a UID number and presents wrong information under their name.	The verification process returns application to the applicant and presents the reasons for not issuing number.
Person applies to get a second card in another name.	Application returned, with reason provided. If person's name was fraudulent the first time, he has the option of applying to change his demographic fields. if this fraud is attempted again, person is added to watch list/ legal action.
Person appears as himself, and applies for a second UID number.	Application returned, with reason provided. If attempted more than three times person added to watch list.
Person appears as another existing person, registering the second person's information under his fingerprint. Impersonation of a deceased individual, with fake supporting documents.	The victim can report identity theft to the UIDAI's grievance office. The UIDAI will undertake an investigation, and take appropriate action if theft is confirmed. If the applicant passes the verification process, then he may be able to take on the stolen identity. However, he will not be able to change his demographic fields over his lifetime without due process.
De-duplication works incorrectly and returns false positive for a new UID applicant.	Person can request check against face biometrics as well as re-verification by Registrar.

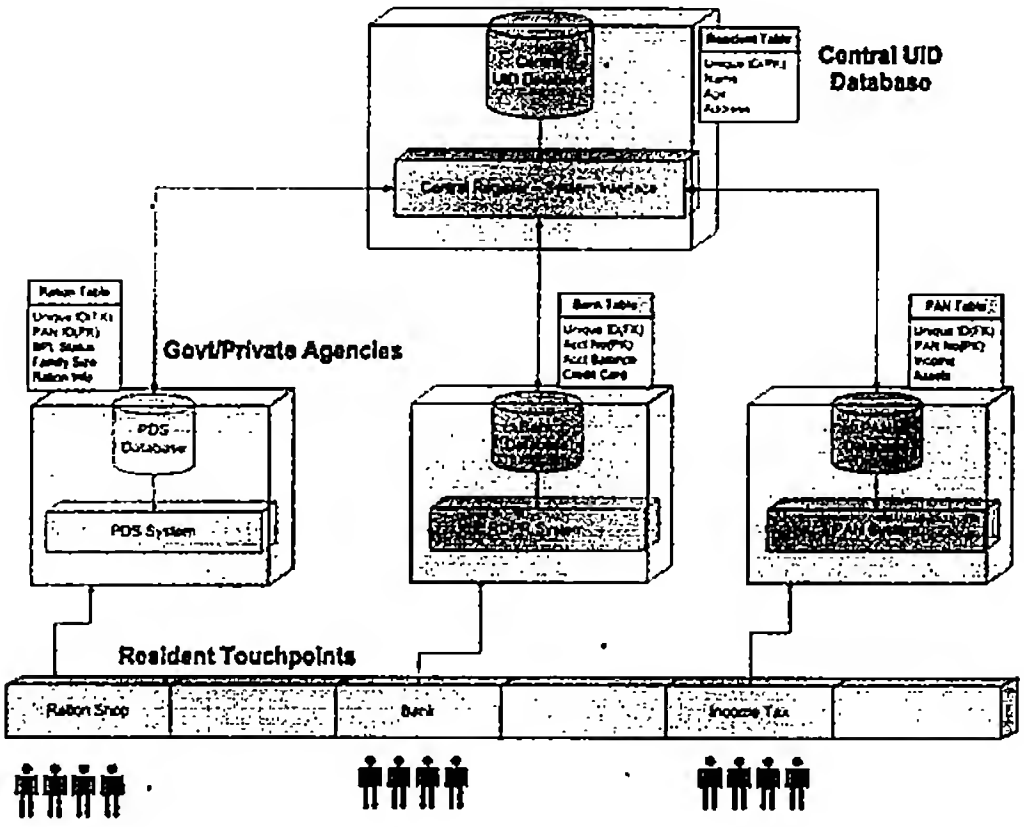
7

Technology architecture of the UIDAI

The technical architecture of the UIDAI is at this point, based on high-level assumptions. The architecture has been structured to ensure clear data verification, authentication and de-duplication, while ensuring a high level of privacy and information security.

7.1 System architecture

The Central ID Data Repository will be the central database of all residents, containing the minimal set of fields sufficient to confirm identity. The federated set of databases belonging to the Registrars may contain additional information about the resident, and can use the resident's UID as the key.



The key technology components of the UID system are:

- The UID Server, which provides the enrolment and the authentication service. These services will be available over the network for the various Registrars and their authenticating agencies to use. The backend servers need to be architected for the high

demands of the 1:N biometric de-duplication as well as the large peak loads from authentication requests.

- The **Biometric sub-system** is central to the UID system for enrolling as well as authenticating residents. It is likely that a multi-modal biometric solution will be used to achieve a high level of assurance. The 1:N de-duplication envisioned will be by far the most computing-intensive operation of the UID system. Innovative techniques of hashing, indexing, distributed processing, and in-memory databases using multiple-biometric-modes need to be employed to get acceptable performance.
- **The Enrolment client** application will capture and validate demographic and biometric data. This client needs to work in an offline mode in the village setting when there is no internet connectivity, and upload batch files to the server for processing. Alternatively the batch files can be physically transported to the CIDR for uploading The client application will be deployed on a standard enrolment workstation.
- **The Network** is a critical aspect of the system, since all UID enrolment and authentication services will be available online. UID services could work over secure WAN networks, the vanilla internet or over mobile SMS channels. It could also potentially work over existing networks such as credit-card POS (point-of-service) devices.
- **The Security design** secures all the above components from logical/physical attack. This includes.
    - Server Security – firewall, intrusion prevention and detection systems (IPS, IDS)
    - Network, Client Security – Encryption, PKI etc
- The Administration system will help administer the UIDAI's operations. This includes
    - Account setup – creation/modification of Registrar, enrolling and authenticating agency accounts.
    - Role based access control – Assign rights over UID resources based on role.
    - Audit trailing – track every access to the UID system.
    - Fraud detection – detect identity theft and cyber crimes using audit trails
    - Reporting and Analytics – Visual decision support tools – GIS, Charting etc.

8

Project Execution

One of the unique challenges in executing the UID project is its scale. Due to the size of India's population, the UIDAI is undertaking what is perhaps the largest governance-related exercise in the world. We must ensure that all aspects of the project – enrolment, de-duplication, and authentication – function effectively even as the number of records approaches a billion.

8.1 Addressing challenges of scale

The UIDAI can expect its enrolment run-rate to have a peak load of one million enrolments per day in the very first year of operation. Every sub-system and component of the UID system will need to scale quickly and significantly. This will include:

1) The ability to onboard Registrars from different sectors and handle their constituencies of residents.

2) The legal framework of contracts needs to support the variety and spread of stakeholders as their numbers grow exponentially across the country.

3) The biometric de-duplication algorithm needs to scale towards checking a fingerprint against every one of 1.2 billion people to ensure uniqueness.

4) The authenticating service, which may be used by tens of thousands of points across the country, needs to scale to handle hundreds of thousands of transactions per second.

9

Project Risk

The UID project does face certain risks in its implementation, which have to be addressed through its architecture and the design of its incentives. Some of these risks include:

1) **Adoption risks:** There will have to be sufficient, early demand from residents for the UID number. Without critical mass among key demographic groups (the rural and the poor) the number will not be successful in the long term. To ensure this, the UIDAI will have to model de-duplication and authentication to be both effective and viable for participating agencies and service providers.

2) **Political risks:** The UID project will require support from state governments across India. The project will also require sufficient support from individual government departments, especially in linking public services to the UID, and from service providers joining as Registrars.

3) **Enrolment risks:** The project will have to be carefully designed to address risks of low enrolment – such as creating sufficient touch points in rural areas, enabling and motivating Registrars, ensuring that documentary requirements don't derail enrolment in disadvantaged communities – as well as managing difficulties in address verification, name standards, lack of information on date of birth, and hard to record fingerprints.

4) **Risks of scale:** The project will have to handle records that approach one billion in number. This creates significant risks in biometric de-duplication as well as in administration, storage, and continued expansion of infrastructure.

5) **Technology risks:** Technology is a key part of the UID program, and this is the first time in the world that storage, authentication and de-duplication of biometrics are being attempted on this scale. The authority will have to address the risks carefully – by choosing the right technology in the architecture, biometrics, and data management tools; managing obsolescence and data quality; designing the transaction services model and innovating towards the best possible result.

6) **Privacy and security risks:** The UIDAI will have to ensure that resident data is not shared or compromised.

7) **Sustainability risks:** The economic model for the UIDAI will have to be designed to be sustainable in the long-term, and ensure that the project can adhere to the standards mandated by the Authority.

10

UID-enabled micro-payment architecture

This section discusses one of the potential applications of the UID – the use of the number in driving financial inclusion, and in enabling a micropayments solution that the poor can use to access financial services.

While the demand for financial inclusion has gained urgency over the last few years, initiatives in India to expand financial infrastructure date back several decades, since the building of rural cooperative credit banks in the 1950s, and the spread of bank networks in the 1970s and 1980s. These initiatives have paid off over the years — India's bank branches are well-networked, particularly across urban India.

But despite these efforts, access to finance has remained scarce in rural India, and for the poorest residents in the country. Today, the proportion of rural residents who lack access to bank accounts remains at 40%, and this rises to over three-fifths of the population in the east and north-east of India.

This exclusion is unfortunate. Economic opportunity is after all, intertwined with financial access. Such financial access is especially valuable for the poor — it offers a cushion to a group whose incomes are often volatile and small. It gives them opportunities to build savings, insure themselves against income shocks and make investments. Such savings and insurance protect the poor against potentially ruinous events — illness, loss of employment, droughts, and crop failures. However due to the lack of access to financial services, many of the Indian poor face difficulties in accumulating savings.

To mitigate the lack of financial access in India, the RBI has focused on improving the reach of financial services in new and innovative ways — through no-frills accounts, the liberalization of banking and ATM policies, and branchless banking with business correspondents2 (BC), which enables local intermediaries such as self-help groups, post offices and kirana stores to provide banking services. These efforts have also included the promotion of core-banking solutions in regional rural banks; and the incorporation of the National Payment Corporation of India (NPCI) as an apex switch, for payments and settlements.

In recent years, ATM and core banking, as well as greater mobile connectivity have also become two powerful engines of financial access. Mobile phones in particular present an enormous opportunity in spreading financial services across India. These technologies have reduced the need for banks to be physically close to their customers, and banks have been consequently able to experiment with providing services through online as well as mobile banking. These options, in addition to ATMs, have made banking accessible and affordable for many urban non-poor residents across the country.

With the poor however, banks face a fundamental challenge that limits the success of these technologies and recent banking innovations. The lack of clear identity documentation for the poor creates substantial difficulties in establishing their identity to banks. This has limited the extent to which we can leverage online and mobile banking to reach these communities.

Besides challenges in access and identity, a third limitation has been the cost of providing banking services for the poor. The poor have unique preferences when it comes to withdrawing money and making deposits — they prefer to do large numbers of small transactions, in 'micropayments' of say, Rs.10 rather than Rs.100. Banks discourage such payments, as transaction costs under this model would be too high to bear. The Unique Identification number (UID), which identifies individuals uniquely on the basis of their demographic information and biometrics, gives individuals the means to clearly establish their identity to public and private agencies across the country. It also creates an opportunity to address the existing limitations in financial inclusion. The UID, once it's linked to a bank account, can help poor residents easily establish their identity to banking institutions. As a result, the UID enables banking institutions to bring together the infrastructure that now exists in order to build an accessible, low-cost micropayments model.

Since the UID enables remote authentication of identity, it empowers the poor in making electronic transactions in small, micro-amounts, remotely and at low-cost, through BC networks connected by mobile phones. The model would thus be accessible and affordable across the country. Such a UID-enabled micropayments approach can bring about universal financial access for the poor — they would be able to access their accounts on the move, wherever they are, through any mobile phone, from any BC or bank. The UID-enabled bank account can thus be a global address for residents, similar to an email id or a mobile phone number.

Over the last few years, we have seen critical reforms implemented towards creating a payments solution for the poor. The UID number helps integrate these reforms and leverage the technology already in place into an effective micropayments solution. This can bring low-cost access to financial services to everyone, a short distance from their homes.

10.1 Features of UID-enabled micropayments

UID KYR sufficient for KYC: Banks in India are required to follow customer identification procedures while opening new accounts, to reduce the risk of fraud and money laundering. The strong authentication that the UID offers, combined with its KYR standards, could remove the need for such individual KYC by banking institutions for basic, no-frills accounts. It will thus vastly reduce the documentation the poor are required to produce for a bank account, and significantly bring down KYC costs for banks.

Electronic transactions: The UID's authentication processes will allow banking institutions to verify poor residents both in person and remotely. Rural residents will be able to transact electronically with each other as well as with individuals and firms outside the village, reducing their dependence on cash.

Ubiquitous BC network and BC choice: The UID's clear authentication and verification processes will allow banking institutions to network with village-based BCs such as self-help groups, post offices and kirana stores. Customers will be able to withdraw money and make deposits at the local BC. Multiple BCs at the local level will also give customers a choice of BCs. This would make customers, particularly in villages, less vulnerable to local power structures, and lower the risk of being exploited by BCs.

A high-volume, low-cost revenue approach: The UID will mitigate the high customer acquisition costs, high transaction costs and fixed IT costs that we now face in bringing bank accounts to the poor.

No-frills accounts that can be provided and accessed at low cost through local Bcs, with electronic cash transfers, would encourage large numbers of small transactions across these accounts, and make these accounts an important source of revenue for banks.

10.2 Benefits

For residents: The UID-enabled Bank Account (UEBA) will bring financial access and affordability to millions of residents who are presently excluded from formal financial systems. A UID-enabled bank account will also help residents make cheaper, faster electronic transactions and remittances in the form of micropayments. The solution will enable universal access to their account from any bank or BC, and through any mobile device, enabling residents to access payments on the move. Regular, affordable access to banking services would also give the poor a means of keeping their money safe — a convenience that has long been available to the middle class would now be accessible to the rural and urban poor.

For the government: Large-scale financial inclusion can pave the way for electronic benefit transfers (EBTs) for residents. Central and state governments will be able to eliminate the identity-related fraud that exists within its public programs with such transfers going into UID-enabled bank accounts. The bulk of the informal cash economy across rural India, and remittances between urban and rural India will also become part of the formal banking system, with traceable and accountable money flows. This will ensure compliance with Anti-Money Laundering laws and Financial Action Task Force standards. The government will gain these benefits without having to overhaul governance systems — the micropayments approach won't require governments to change decision-making processes across the central, state and local level.

For banking institutions: The use of the central payments switch to move cash electronically at the last mile will dramatically cut down on cash handling and transaction costs for banking institutions. The cost of customer acquisition would also be significantly reduced, as a resident with a UID would require no further identification to get a UID-enabled bank account.

A low-cost micropayment approach will make the large volume of micropayments, remittances and government transfers to UID-enabled bank accounts important sources of revenue for banking institutions. Through the BC network, banks would be able to access customers through

the large distribution channels in the country — including the mobile prepaid network, post office network and FMCG retailers. In addition, BCs would see increased revenues from larger numbers of micro-transactions.

10.3 Conclusion

Over the last decade, we have seen a transformation in financial access for residents across the country — the reforms that encouraged the expansion of ATM, internet and mobile banking have made financial access affordable and accessible for large numbers of residents.

The transformation however, has been most significant for India's urban, non-poor residents. These policies have not addressed the unique challenges the poor face in financial access, and they consequently, remain at the periphery when it comes to effective access to finance.

The UID-enabled micropayments solution is just one of the many developmental applications that the UID number can enable. It is also a critically important application, which can help address India's financial divide. Linking the UID number to a universal, accessible, and affordable micropayments model can transform the access the poor have to banking services in the country.

UID-enabled micropayments can be a stepping stone to creating economic opportunities for residents across the country, regardless of where they live. The financial inclusion that it makes possible will be critical to improving access for the poor to resources and skills. As we move towards an open access society, it is this soft infrastructure — connectivity, financial inclusion, and identity — that will ultimately, empower the individual in India.

ANNEXURE-B

DATA SHARING POLICY

UIDAI embarked on a multi-Registrar model for enrolling the residents with the intent to have the reach and ability to enrol the residents at a reasonable pace.

Registrars are entities who, in the normal course of their activities, deal with residents in the delivery of benefits and services to them. The Registrars carried out enrolments under the aadhaar project through Enrolment Agencies appointed by them. These Registrars already have data bases and collect data from their customers/beneficiaries for discharging the responsibilities cast up on them under various policies, statutes or rules. The Registrars partnered with the UIDAI to avail the opportunity of cleansing their data bases through fresh enrolments of residents in accordance with the UIDAI processes.

In some States where the non-State Registrars were active, State Registrars are facing problems in leveraging aadhaar for delivery of benefits (which is the basic intent of aadhaar project) since data of residents of the State enrolled by the non-State Registrars was not available to the State Registrars. Many State Registrars have had reservations about the involvement of Non State Registrars in the enrolment exercise in absence of any clarity as to how they would be able to access the data of residents enrolled by Non State Registrars. The Enrolment Refresh Committee had also mentioned about the need of sharing of data with such Registrars.

In such a scenario, a policy on data sharing policy assumes an important dimension; wherein on one side, there are concerns regarding privacy, data protection, data security, etc, and on the other hand, there is demand from various State Registrars for the data to enable them leverage the UID for improving the services.

With the above in consideration, it has been decided that UIDAI would share the Resident data, subject to the following conditions:

1. UIDAI would share the data only in such cases where the resident has given the consent for sharing data.
2. The data will be UID generated processed data.
3. The data will be shared on receipt of a formal request from the State concerned. The request will explicitly include the purpose for which the data is required and specific data requirements.
4. States may request data pertaining to their own state only. The data shared will be based on state specified in the resident address.
5. The selective data in specific format, as defined by UIDAI, will be shared as per the validity of the request in a secured manner using appropriate offline and/or online mechanisms.
6. The data would be shared with State Registrars only for the purpose of improvement of delivery of welfare and public services, it also being the intent behind the aadhaar project and the purpose for which the consent has been given by the resident at the time of enrolment.

196

7. Demographic data may be shared with Financial Institutions (Banks, etc) for opening of Bank accounts and/or linking the accounts with aadhaar, as consented by the resident at the time of enrolment or subsequently.
8. Data may also be shared as warranted under any Act/ Statute/ Regulation of Govt of India and/or any Cabinet Decision in this regard.
9. State Registrars may use the shared data with their various departments for the purpose of improving delivery of their welfare and public services but the Nodal Department shall be responsible for ensuring Security compliance.
10. The Registrar packet will not be generated, if Registrar does not ask for it.
11. UIDAI may also consider enabling electronic KYC mechanism where an authorized entity can send a request to UIDAI to share demographic data and photo for a specific resident, in the long run. This mechanism will require the said entity to send resident data sharing consent along with resident authentication factor (biometric/OTP). UIDAI will share data after successful resident authentication. UIDAI will define set of authorized entities who will be allowed to avail this service, at the appropriate time.
12. Updates should be allowed to flow to agencies with whom UIDAI shared the data initially as per resident consent from time to time.
13. The necessary framework and institutional safeguards as per the IT Act 2000 and all guidelines/rules/enactments of the Government of India for ensuring the data safety and security at all times would be put in place by concerned Registrar before sharing of any data. Registrar will sign a *"Data protection and Understanding of holding sensitive data"* agreement with UIDAI. Among other things, the Agreement will include various required compliances for the following security guidelines and any other security guidelines as the UIDAI may deem fit:-
    a. Strategic control of the data shall always remain with the Registrar who shall be responsible for the overall security and proper use of the data at all times.
    b. Data shall be stored and transmitted in encrypted form.
    c. Biometric data shall not be decrypted except for the time when it is being used. Under no circumstances, the biometric data of a resident shall be sent as part of any response to any verification request.
    d. Registrar shall have a physically secure location to store /house the shared data, with strict security protocols and protection from unauthorised access. The facility should have appropriate access control and audit trails.
    e. Physical, Network and Application level security for the software that uses this data shall be ensured.
    f. State Registrar shall remove the biometric data if "resident" moves out of the state and informs the state.
    g. The data should not be retained beyond the duration necessary to serve the purpose for which it was meant to be used.
    h. Failure to comply with any of above obligation shall be deemed a serious breach by the Registrar concerned with whom data was shared by UIDAI and the said Registrar shall destroy the shared data within the time specified by UIDAI, without prejudice to any damages, which UIDAI may seek.

Data Protection and Security Guidelines for Registrars

1. Background

This document lays down the data protection and security guidelines to be followed by Registrars of the Unique Identification Authority of India (UIDAI). Since the Aadhaar enrolment process and the enrolment for the services of the Registrar is common, it is essential to define the parameters of responsibility of UIDAI and the Registrars.

There are two components to the enrolment process:

a) **Enrolment for Aadhaar** – for which the resident provides their name, date of birth, gender, address and other optional fields such as mobile number , e-mail etc along with biometrics, namely, Photograph, 10 Finger prints and Iris. UIDAI will be responsible for safe custody of the information collected for the purpose of Aadhaar generation once it reaches CIDR.

b) **Enrolment for the Registrars services** – In addition to the information being collected by UIDAI, the Registrars may also be collecting a wide range of information together with biometrics and the Aadhaar number in order to deliver their services to the residents. This information could be viewed as personal information. Hence, ensuring the confidentiality and security of this data is of great importance.

2. UIDAI responsibility for - data protection and security

UIDAI is capturing biometrics and demographics information to issue Aadhaar numbers to the residents and to authenticate the identity of an Aadhaar number holder. It is the responsibility of UIDAI to ensure safety and security of the data collected for Aadhaar enrolment. The data captured (demographic and biometric) shall at the point of collection be encrypted and transported to the Central Identities Data Repository where the UIDAI will decrypt the data in a secure location and use it for the purpose of de-duplication and subsequently for authentication. UIDAI will have a security policy in place which will detail and define the security protocols and access protocols to ensure safety of the data. It is the responsibility of the UIDAI to ensure the safety, security and confidentiality of the data from the point of receipt and in the CIDR and to protect the data from unauthorised access and misuse.

3. Registrars responsibility for – data protection and security

The Aadhaar enrolments will be done through the Registrars. The Registrars will also be collecting additional data from the resident in order to deliver their services to the resident. This relationship between the resident and the Registrar is independent of the UIDAI. As a consequence Registrars have a fiduciary responsibility and has to exercise a duty of care to secure and protect all the data (demographic and biometric) collected from the resident. UIDAI prescribes the following broad measures for data protection and security to be adopted by Registrars:

a) Care in collection:
   - Registrars shall take all necessary precautions, in respect of information received or collected by it so as to ensure such information is properly and accurately recorded, collated and processed;

b) Process for access and updating:
   - Registrars shall also establish and adopt procedures to disclose to a person, upon their request, their own information – subject to satisfactory identification (in order to ensure that information is not revealed to third parties)

c) Principles and procedures relating to data collection, use and processing
   - Registrars must collect information from residents only for the purpose related to their functions.
   - The individual from whom data is being collected should be informed of the purpose for which information is being collected and how the data will be used.
   - Registrars should obtain appropriate and clear legal consent from the resident.
   - Registrars must ensure that data collected and maintained by them is protected against any loss, or unauthorized access, or use, or modification or disclosure.
   - Data provided by the resident to a Registrar should be used by the Registrar for the purpose envisaged. Resident must be made aware of any data sharing policies of the Registrar. While some form of sharing maybe part of the governance framework of governments – residents must be made aware of the same. Any other sharing beyond the governance framework must only be done with the explicit consent of the resident and for the explicit reason for which the consent is given.

d) Data security protocols

- Security protocols should be in place from the point of collection, transmission of data and to the final destination/ facility where the data will be stored.
- Data must be housed in a secure facility with appropriate access controls and audit trails.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful collection and processing of data and against accidental loss or destruction of, or damage to data.

e) Data retention policy

- Registrars must define the time period for which data is being collected and will be retained by them. Data should not be retained for longer than the purpose for which it was meant to be used.
- Data must not be made available for the use of or be retained by third party service providers such as enrolling agencies or by any other unauthorised personnel.
- Registrars must develop their own guidelines for preservation and destruction of data and records according to their functional needs.

4. Security framework for Biometric data

While the above broad guidelines are applicable for all forms of data collected from the residents, special care needs to be taken to address the security of biometric information. Biometrics is unique to an individual and therefore is sensitive information that needs to be protected with the highest standard of care to thwart any possibility of misuse.

The biometric data will be encrypted immediately upon capture during the enrolment process. The data packet will be encrypted with the Registrars key. The Registrar is responsible for the secure transmission of the data and for storing the data at a secure location protected from unauthorised access and misuse. The Registrar is liable to the resident and the public at large for safety, security and proper use of the Biometric data collected by it. The following guidelines are prescribed for the Registrars for security protocols relating to biometric information of the residents.

4.1 Guidelines

1. Registrars should inform residents what biometric data is being collected and how the data will be used.

2. Develop data use and retention policies - Registrars should not collect and retain more data than they need for their purpose (if they want to issue cards

and store finger print they should retain that data only and not the rest). Information that is not required must not be retained by them.

3. Registrars should develop data security policies and build up systems to ensure safe keeping of biometric data, protect from malware, spyware and hacking of systems, including access protocols, etc. For this purpose :
   - Registrars must have a physically secure location (data centre) where the biometric data can be housed, with strict security protocols and protection from unauthorised access. Physical, network and application security must be taken care of.
   - Biometric Data should always be stored in encrypted form. Data should not lie unencrypted at rest.
   - Biometric Data should not be decrypted except for the time when it is being used.
   - Only data that is required should be retained and the rest should be destroyed.
   - Key management systems with logging and audit trails should be created preferably using a Hardware Security Module (HSM).
   - Independent audit of the security facilities, processes and policies should be done periodically and reports should be published to assure the public of the safety standards being followed.

4. Biometric data should not be made available to or be retained by enrolling agencies, at user points or by any other unauthorised personnel.

5. Key technical safeguards

Overall objective

To ensure that all UIDAI Registrars meet a minimum level of security when they store, process and transmit resident data the UIDAI has prescribed following control objectives and recommendations to meet them :

Control Objectives	UIDAI Recommendations
Maintain an Information Security Policy	Maintain a policy that addresses information security
Maintain a Vulnerability Management Program	Use and regularly update anti-virus software on all systems commonly affected by malware
	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	Restrict access to resident data by business need-to-know
	Assign a unique ID to each person with

	computer access
	Restrict physical access to resident data
Build and Maintain a Secure Network	Install and maintain a firewall configuration to protect resident data
	Do not use vendor-supplied defaults for system passwords and other security parameters
Regularly Monitor and Test Networks	Track and monitor all access to network resources and resident data
	Regularly test security systems and processes
Protect Resident Data	Protect stored resident data
	Encrypt transmission of resident data across open, public networks

Maintain an Information Security Policy

Registrars must create and maintain an information security policy, which addresses the security requirements arising out as a result of their functional/ business needs and objectives. The objectives of this security policy are to:

- Provide management direction and support for information security.
- Provide a baseline for information security. Partner will have the flexibility to modify components of the operational framework to take into account specific business objectives and security requirements.
- Ensure appropriate safeguards and procedures are adopted to protect information and associated information technology resources
- Ensure that persons handling information are aware of their accountability and responsibilities

This policy shall be implemented through a process approach, based on the PDCA (Plan, Do, Check, Act) as follows. Sample Policies and Procedures followed by other organizations are listed in the annexure .

- **Plan**
  Establish a security policy, objectives, targets, processes and procedures relevant to managing risk, and information security to deliver results in accordance with the Partner's overall policies and objectives
- **Do**
  Implement and operate the security policy, control processes and procedures.
- **Check**
  Monitor, and review the Security policy, control processes and procedures

- **Act**
  Take corrective and preventive actions based on audit and review to achieve continuous improvements of the security plan.

Maintain a Vulnerability Management Program

Registrars must formulate risk assessment policies, and procedures. As a part of this, all assets must be listed, threats & vulnerabilities identified, and assessed, and mitigation plan implemented for all threats. As a result of this, all vulnerable and high risk components would be identified, and protected. Some specific recommendations that may come out of such an exercise include:

- Use and regularly update anti-virus software on all systems commonly affected by malware. This includes all anti-spyware, anti-virus, and other host protection systems.
- Develop and maintain secure systems and applications. This includes the adoption of a secure software development life cycle.

Implement Strong Access Control Measures

Registrars must identify all information assets, and how they are used in their system. This must be followed by the following actions:

- Restrict access to resident data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to resident data

Access control must include physical, host (computer), and network security.

Build and Maintain a Secure Network

It is essential that a secure network be established to protect the system from attack, and misuse. Some sample guidelines for securing this network include:

- Install and maintain a firewall configuration to protect resident data. A firewall is required to prevent external, potentially malicious intruders from accessing the network, and the resources within.
- Do not use vendor-supplied defaults for system passwords and other security parameters. A commonly ignored aspect of security is that various systems come with default security parameters including passwords. Having them set to default values would allow intruders to access the network, and steal data / inflict damage.

Regularly Monitor and Test Networks

Once a secure network is established, it must be regularly monitored, and steps must be taken to keep it up-to -date for all security issues. Some possible mechanisms to ensure this include:

- Track and monitor all access to network resources and resident data
- Regularly test security systems and processes
- Regular security audits, and penetration tests for all systems, networks, and processes will help to keep security up to date with current threats, and ensure that no complacency sets in.

Protect Resident Data

From the resident's perspective, the primary purpose of all security plans is to ensure that the resident's data is not stolen, vandalized, or compromised in any way. To accomplish this, in addition to all the previous steps, the Registrar must classify resident data based on value, and usage. Further, a cryptographic system must be put in place

- Encrypt resident data at rest: i.e. all resident data must be encrypted, while it is stored on external or internal secondary storage.

- Encrypt resident data in motion: i.e. all resident data must be encrypted while it is being transmitted across open public networks (or even closed networks).

- Protect unencrypted data: i.e. while the data is in the host memory, unencrypted, the host system must be protected from malicious activity, including viruses, spyware, etc.

6. Compliance

Compliance can be summarized into 3 stages:
Collecting and storing: Secure collection and tamper-proof storage of all log data so that it is available for analysis.

Reporting: Being able to prove compliance on the spot if audited and present evidence that controls are in place for protecting data.

Monitoring and alerting: Have systems in place such as auto-alerting, to help administrators constantly monitor access and usage of data. Administrators are warned of problems immediately and can rapidly address them. These systems should also extend to the log data itself – there must be proof that log data is being collected and stored.

Compliance can be accessed through the use of an annual onsite data security audits, and quarterly network scans.

Annexure : List of Sample Policies which the Registrars must have in place:

- Information Security & Management Policy
- Information Security Organization Structure Policy
- Risk Assessment Policy & Procedures
- Asset Classification Policy and Procedure
- Asset Classification and control standard
- Information labeling and handling procedure
- Acceptable Use Guideline
- Procedure for control of documents and records
- Human Resources Security Policy and Procedure
- Physical and Environmental Security Policy and Procedure
- Change Management Policy and Procedure
- Third Party Management Policy and Procedure
- Antivirus and Malicious Software Policy and Procedure
- Backup and Restore Policy and Procedure
- Network Security Policy and Procedure (Including internet, intranet, mobile computing, tele-working, firewall security)
- Media Handling Policy and Procedure
- Monitoring Policy and Procedure
- Access Control Policy and Procedure (including password security)
- Network Access Control Policy and Procedure
- Systems Development Maintenance Policy and Procedure
- Incident Management Policy and Procedure
- Business Continuity Management Policy and Procedure
- Cryptographic procedure document
- Minimum Baseline Security Standards

UIDAI

Unique Identification Authority of India
Planning Commission, Govt. of India (GoI),
3rd Floor, Tower II,
Jeevan Bharati Building,
Connaught Circus,
New Delhi 110001

205

Policy on Permanent Centre Model

206

Table of Contents

UD 1. Document Statistics

Type of Information	Document Data
Title	Policy on Permanent Centre Model
Document Revision #	
Document Owner	Anil Khachi, Deputy Director General
Document Author(s)	Pragati Rawat – PMU
Document Reviewer(s)	Kim Kipgen, Assistant Director General

UD 2. Introduction

Aadhaar is a 12 digit unique identification number issued by the Unique Identification Authority of India on behalf of the Government of India, to every resident who enrolls for it.

Any individual, irrespective of age and gender, who is a resident of India and satisfies the verification process laid down by the UIDAI can enroll for Aadhaar. Each Aadhaar number will be unique to an individual and will remain valid for life. The uniqueness is assured through de-duplication of resident's demographic & biometric information. The number itself is bereft of any intelligence and avoids profiling the individual.

Aadhaar number is expected to provide access to a host of services like banking, mobile phone connections and other Government and Non- Government services in due course. This number is expected to serve as a proof of identity and address, anywhere in India.

UIDAI has partnered with a number of entities already engaged in delivery of some public/welfare service to the residents. They are known as Registrars. The Aadhaar (UID) number being a unique, life time number, requires the information contained in the Aadhaar database to be regularly updated. Definition of an Update, in this context, is any modifications to the demographic or biometric data of a Resident including biometric exceptions. The need for such updates can arise from events such as relocation to a new place, age progression, lifecycle changes such as marriages, deaths etc.

UD 3. Need for Permanent Centre

Permanent enrolment centres are required to facilitate the enrolment of residents left out in the camps organized by the Registrars in the past. They would also serve as Update Centres - both for biometric and demographic update. These centres will have all the devices & enrolment client required for doing enrolments as well as Demographic and Biometric Updates. These permanent enrolment centres will have to adhere to all the prescribed processes and guidelines issued by UIDAI regarding fresh enrolment as well as update, and will have to carry out their work only through software and hardware prescribed by UIDAI for this purpose.

These Permanent Centres will be known as "Aadhaar Kendra".

Aadhaar Kendras can be utilized in more than one ways. Apart from enrolments and updates, these Kendras can also be used for other services like finding the status of Aadhaar enrolments, e-Aadhaar letter printing and Lost UID enrolments.

Need for fresh enrolment as well as update of data arise on account of the following reasons:

UD 3.1 New Enrolments

a) The population that could not be covered in the initial enrolment camps needs to be given an opportunity to get enrolled into Aadhaar.
b) New born will also be require a facility to be enrolled for Aadhaar.

UD 3.2 Need for Biometric Updates

a) Age <5 years at the time of initial enrolment – Currently, all children below the age of 5 years only have their demographic data recorded. No biometrics are collected in their case and their identity is tagged to one of their guardians, who must have enrolled for Aadhaar. The child requires to be reenrolled when the child attains age of 5 years and all biometric data should be provided. A PoA, PoI & DoB verification mechanism similar to the one followed during enrolment process would need to be followed. A de-duplication would be done for the child at this stage although the Aadhaar number will remain the same.
b) Age 5-15 years at the time of enrolment – All residents above the age of 5 years are enrolled with their biometrics, but since the biometrics, especially the fingerprints undergo some changes, UIDAI requires all such residents to furnish all biometrics for updates when the resident attains age of 15 years.
a) Age >15 years at the time of enrolment – Residents are recommended to update their Biometric data every 10 years.
b) Events like accidents or diseases leading to biometric exception
c) As the Aadhaar authentication service becomes ubiquitous, residents may also approach for biometric updates because of authentication failures which may result from incorrect biometric capture or poor biometric quality captured at the time of enrolment. With improvements in technology, it may be possible to capture better quality biometrics in the CIDR.

UD 3.3 Need for Demographic Updates

a) Changes in life events such as marriage may lead to residents changing their basic demographic details such as name and address. Address and mobile number could also change due to migration to newer locations. Residents may also want changes in their relative's details due to changes in life events such marriage, death of a relative etc. In addition, residents could have other personal reasons to change their mobile number, email address etc.

b) Changes in various service delivery platforms may lead residents to request changes to "information sharing consent", and to add mobile number to CIDR etc.

c) Any errors made during the enrolment process wherein the resident's demographic data may have been captured incorrectly.

UD 4. Various Models for Permanent Centres

The current enrolment model of UIDAI permits Registrars to either enrol residents itself or else engage professional enrolment agencies. Similarly, there are a number of options available to the Registrars to set-up and operate Permanent Enrolment Centres.

UD 4.1 Permanent Centre Setup run by State Governments / Registrars

a) Located in the government buildings in block/mandal/tehsil/municipal ward office/

Or in the official premises of the Registrar

b) Laptop and scanner, printer, GPS device and other UIDAI prescribed devices procured by the State Government/Registrar. The balance funds available to the Registrars from the Enrolment support provided for successful Aadhaar generation can also be utilized for this purpose.

c) Staffing options
   - Existing staff trained and certified to take extra responsibility of operator / supervisor with honorarium payment. The amount is to be decided by the Registrar/ State government.
     or
   - Operators hired on contract basis and Verifier/Supervisor role undertaken by office staff

d) The State Government/Registrar may choose to bear the expenses at these Centres and provide Update services free to the resident. They can fund these expenses out of the balance funds available to the Registrars from the Enrolment support per successful Aadhaar enrolment and the funds provided by UIDAI for successful biometric updates.

e) Alternatively they may charge convenience fee from the residents, as suggested by UIDAI in section 4.

UD 4.2 Outsourced by the State Government / Registrars to 3rd Parties

a) Contract provided to the private partner for setting up a permanent enrolment centre by State Government /Registrar. Registrar's/State Government may use the existing empanelled Enrolment Agencies of UIDAI. However, the locations will be pre-defined and static and will be declared as a part of the Permanent Centre on-boarding exercise before the service is rolled out.

b) Fee model for updates- residents are charged a nominal fee to cover the cost of running the permanent enrolment centre. UIDAI has suggested the convenience fee that can be charged from the residents in section 4 of this document.

c) Support for enrolment of residents for the first time (New Enrolment) would be available from UIDAI strictly on outcome basis i.e on successful generation of Aadhaar and as per approval of the Govt. of India, from time to time.

d) The Regional Offices of UIDAI will continue to play the role of inspection, technical support and coordination for the permanent centres. ROs will on-board the Registrars.

UD 5. Guidelines on Payment Policy for Updates

- UIDAI will bear only the cost incurred for back end processing of update requests, cost on account of verification/approval at the back-end, sending of Aadhaar letters and other costs at the back-end. The residents will not be charged for these till March 2014. The Government of India may review the proposal thereafter.
- For all update requests, demographic and/or biometric, where the resident visits the centre for updates, a convenience fee of Rs. 15/- per request can be charged from the residents. Alternatively, the Registrars may bear this cost and keep the updates free for residents.
- Additionally, financial assistance @ of Rs.20/- per successful biometric update will be provided by UIDAI.
- The policy will be reviewed after March 2014, and a suitable business/pricing model would be announced thereafter.
- Charges for other services such as printing e-Aadhaar have been separately approved by UIDAI.

Registrars need to come up with IEC strategies and encourage Aadhaar application in various government schemes for customers in the voluntary updates category to be able to perceive value in paying for data update.

UD 6. Setting up of Permanent Centre

Registrars need to prepare in terms of infrastructure, personnel, process and technology for setting up permanent enrolment centres. Registrars must ensure that the following responsibilities can be discharged before commencing any enrolment/update activity and provide a letter of acceptance for these to the Regional Office of UIDAI:

a) The Permanent Enrolment Centres/Stations will also function as update centres.
b) The Permanent Enrolment Centre location plans will be shared with the respective Regional Offices of UIDAI and uploaded on the Permanent Enrolment Centre portal of UIDAI.
c) Duly completed Registrar Readiness Checklist will be submitted to obtain a sign off from the respective RO. The actual enrolment/updation may be commenced under intimation to the Regional Office of UIDAI.
d) Only trained & certified Operators/Supervisors shall be engaged for enrolment/update activities.
e) Operators/Supervisors must have their Aadhaar number before undertaking any enrolment/update.
f) Registrar and its Operators/Supervisors must be fully conversant with all the prescribed processes/guidelines & standards for enrolment of residents under the Aadhaar project and update of their data. The Registrar and its EA will strictly adhere to these instructions/guidelines/processes issued from time to time.
g) Data Security Guidelines prescribed for Registrars and EAs and their Operators/Supervisors will be adhered to at all times.
h) The Registrar must be conversant with the various policies put in place including Suspension Policy, Data and Process error Penalties, Document Management System, Training & Certification of Operators/Supervisors, PINCODE Management etc.
i) Only certified devices of the approved specifications will be deployed. The Registrar will also ensure timely migration to newer version of the enrolment/update client as per UIDAI's instructions.
j) The approved introducers & verifiers will have to be notified.
k) Synchronization of enrolment Stations will have to be ensured every 10 days.
l) Uploading of enrolment packets regularly and not later than 20 days from the date of enrolment must be ensured.
m) Ensure proper indexing, custody and safe keep of the enrolment/update related documents.
n) Monitoring the permanent Centre regularly.
o) No financial support other than the ones mentioned in guidelines for payment section would be extended by UIDAI for these centres.
p) The State Govt./UT would be at liberty to fix reasonable rates for update of information provided by a resident for Aadhaar enrolment and no financial support shall be provided by UIDAI for any update of information barring successful biometric update as referred in para 5 "Guidelines on Payment Policy for Updates" above.

UD 7. Reference Checklists and Process Documents

UIDAI has published Data Update Policy and process for Update using Update Client. Apart from these, there are checklists and process documents that Registrar must be aware of and comply.

Refer the following checklists and process documents for getting ready:

1. **Registrar Readiness Checklist for Permanent Centres** - During the initiation and planning stage, use this checklist.

Microsoft Office Excel 97-2003 Worksl

2. **Enrolment Centre Setup Checklist** - This checklist lists all mandatory & desired hardware/software and other requirements at an enrolment centre.

Adobe Acrobat Document

3. **Checklist for personnel** – Refer Roles and Responsibility documents for Operator, Supervisor, Verifier and Introducer, attached respectively.




Microsoft Office Word 97 - 2003 Docu | Microsoft Office Word 97 - 2003 Docu | Microsoft Office Word 97 - 2003 Docu | Microsoft Office Word 97 - 2003 Docu

4. **Resident Enrolment Process** – Refer latest Resident Enrolment Process document under "Process Manuals and Guidelines" on page **http://www.uidai.gov.in/registrar-link-2.html**

5. **Update Policy and Process** – Refer latest Update Policy and Process through UCS mode under "Process Manuals and Guidelines" on page **http://www.uidai.gov.in/registrar-link-2.html**

UD 8. Number of Station requirement/sub-district, for the pilot districts, based on population

Registrars should plan for setting up Permanent Enrolment Centres to facilitate on-going enrolments and update. Long term/Permanent enrolment stations need to be established by the Registrar at Taluk/Block/Municipality level. UIDAI suggests that there should be at least one centre/ sub-district to cover the sub-district population. The Registrar can plan for more than the indicated numbers. Refer the table given below for suggested minimum station requirement/sub-district based on district population.

S. No.	State	District	No. of Sub-Districts	No. of Permanent Enrolment Stations Recommended
1	Andhra Pradesh	Ananthapur	63	68
		Chittoor	66	70
		East Godavari	59	86
		Hyderabad	16	67
		Rangareddy	37	88
2	Chandigarh	Chandigarh	1	18
	Daman and Diu	Daman	1	3
		Diu	2	2
3	Delhi	North East Delhi	2	37
4	Delhi	North West Delhi	6	61
5	Goa	North Goa	6	14
6	Gujarat	Anand	8	35
		Bhavnagar	11	48
		Mahesana	9	34
		Valsad	5	28
7	Haryana	Ambala	3	19
		Sonipat	4	25
8	Himachal Pradesh	Bilaspur	5	6
		Hamirpur	6	8
		Mandi	16	17
		Una	5	9
9	Jharkhand	Hazaribag	11	29
		Ramgarh	4	16
		Ranchi	16	49
		Seraikela-Kharsawan	7	18
10	Karnataka	Dharwad	4	31
		Mysore	7	50
		Tumkur	10	45

S. No.	State	District	No. of Sub-Districts	No. of permanent Enrolment Stations recommended
11	Kerala	Pathanamthitta	6	21
		Wayanad	3	14
12	Madhya Pradesh	Harda	3	10
		Hoshangabad	7	21
		Khandwa	5	22
13	Maharashtra	Amravati	14	48
		Mumbai	33	208
		Nandurbar	6	27
		Pune	15	157
		Wardha	8	22
14	Puducherry	Pondicherry	6	11
15	Punjab	Fatehgarh Sahib	4	10
		Gurdaspur	5	38
		Shaheed Bhagat Singh Nagar	2	10
16	Rajasthan	Ajmer	9	43
		Alwar	12	61
		Udaipur	10	61
17	Sikkim	East Sikkim	3	5
		West Sikkim	2	2
18	Tripura	Dhalai	5	6
		North Tripura	9	12
		South Tripura	10	15
		West Tripura	18	29
	TOTAL		585	1834